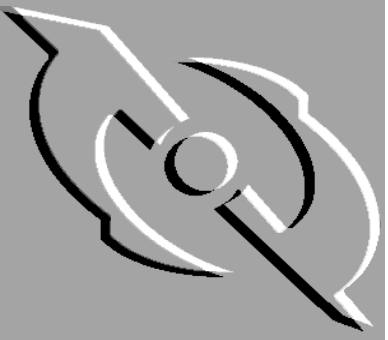


GroupShield für Exchange

Administratorhandbuch

COPYRIGHT

Copyright © 1998-2000 Network Associates Technology, Inc. Alle Rechte vorbehalten. Kein Teil dieser Veröffentlichung darf ohne schriftliche Erlaubnis von Network Associates Technology, Inc., ihren Lieferanten oder zugehörigen Tochtergesellschaften in irgendeiner Form oder mit irgendwelchen Mitteln vervielfältigt, übertragen, transkribiert, in einem Informationsabrufsystem gespeichert oder in eine andere Sprache übersetzt werden. Um diese Genehmigung zu erhalten, schreiben Sie bitte an die Rechtsabteilung (Legal Department) von Network Associates unter folgender Adresse: 3965 Freedom Circle, Santa Clara, California 95054, USA. Oder rufen Sie +1 972 308-9960 an.

LIZENZVERTRAG

HINWEIS FÜR ALLE BENUTZER: SPEZIELLE BESTIMMUNGEN IHRER LIZENZ ZUR VERWENDUNG DER SOFTWARE, DIE DIESE DOKUMENTATION BESCHREIBT, FINDEN SIE IN README.1ST, LICENSE.TXT ODER IN EINEM ANDEREN LIZENZDOKUMENT, DAS IHRER SOFTWARE ALS TEXTDATEI ODER IN DER SOFTWAREPACKUNG BEILIEGT. INSTALLIEREN SIE DIE SOFTWARE NICHT, WENN SIE NICHT ALLEN HIERIN ENTHALTENEN BESTIMMUNGEN ZUSTIMMEN. IN DIESEM FALL KÖNNEN SIE DAS PRODUKT GEGEN VOLLE RÜCKERSTATTUNG DES KAUFPREISES DER STELLE ZURÜCKGEBEN, VON DER SIE ES ERHALTEN HABEN.

NETWORK ASSOCIATES MARKENRECHTE

* *ActiveHelp, Bomb Shelter, Building a World of Trust, CipherLink, Clean-Up, Cloaking, CNX, Compass 7, CyberCop, CyberMedia, Data Security Letter, Discover, Distributed Sniffer System, Dr Solomon's, Enterprise Secure Cast, First Aid, ForceField, Gauntlet, GMT, GroupShield, HelpDesk, Hunter, ISDN Tel/Scope, LM 1, LANGuru, Leading Help Desk Technology, Magic Solutions, MagicSpy, MagicTree, Magic University, MagicWin, MagicWord, McAfee, McAfee Associates, MoneyMagic, More Power To You, Multimedia Cloaking, NetCrypto, NetOctopus, NetRoom, NetScan, Net Shield, NetShield, NetStalker, Net Tools, Network Associates, Network General, Network Uptime!, NetXRay, Nuts & Bolts, PC Medic, PCNotary, PGP, PGP (Pretty Good Privacy), PocketScope, Pop-Up, PowerTelnet, Pretty Good Privacy, PrimeSupport, RecoverKey, RecoverKey-International, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, Site Meter, Sniffer, SniffMaster, SniffNet, Stalker, Statistical Information Retrieval (SIR), SupportMagic, Switch PM, TeleSniffer, TIS, TMach, TMeg, Total Network Security, Total Network Visibility, Total Service Desk, Total Virus Defense, T-POD, Trusted Mach, Trusted Mail, Uninstaller, Virex, Virex-PC, Virus Forum, ViruScan, VirusScan, VShield, WebScan, WebShield, WebSniffer, WebStalker WebWall* und *ZAC 2000* sind eingetragene Marken von Network Associates und / oder Tochterfirmen in den USA und / oder anderen Ländern. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind das alleinige Eigentum der jeweiligen Inhaber.

Inhalt

Preface xi

Virenschutz ist Datensicherheit xi
Informationssicherheit als Geschäftsnotwendigkeit xiv
Active Virus Defense-Sicherheitsperipherie xv
Auf Ihrem Microsoft Exchange-Server xvi
McAfee-Virenschutzforschung xvii
So nehmen Sie Kontakt zu McAfee und Network Associates auf xvii
Kundendienst xvii
Technischer Support xix
Support für Herunterladen xx
Network Associates-Schulung xx
Kommentare und Feedback xx
Melden neuer Posten für Virenschutzdatendateien xxi
Internationale Kontaktinformationen xxii

Kapitel 1. Willkommen bei GroupShield für Exchange 27

Der Lieferumfang GroupShield für Exchange 28
Wichtigste Features von GroupShield für Exchange 30

Kapitel 2. Erste Schritte 31

Bevor Sie beginnen 31
Lieferumfang von GroupShield für Exchange 31
Rechte and Berechtigungen 31
Serveranforderungen 32
Sonstige Voraussetzungen 32
Installationscheckliste 33
Installieren von GroupShield für Exchange 34
Testen einer Installation 44
Änderungen am System nach Abschluß der Installation 46
Ergänzende Informationen 47
Globale Formulare von GroupShield für Exchange 47

Die Quarantäneorte 48
Anfordern von Hilfeinformationen über GroupShield für Exchange . . .48
Beenden und Neustart der Dienste 48
Öffnen der Serververwaltungskonsole GroupShield-Eigenschaften . .50
Aktualisieren von GroupShield für Exchange 51
Reparieren der Software 54
Entfernen der Software mit dem Windows Installer 56
Manuelles Entfernen der Software 57

Kapitel 3. Scanvorgänge „bei Zugriff“ 61
Scanoptionen 62
Festlegen der Aktionen zur Behandlung aufgespürter Viren 65
Blockieren von Anlagen bestimmten Typs 66

Kapitel 4. Scanvorgänge auf Anforderung 71
Konfigurieren von Scanvorgängen auf Anforderung 72
Auswahl der zu scannenden Objekte 72
Scanoptionen 76
GroupShield für Exchange-Aktionen bei Viruserkennung 79
Scannen neuer oder geänderter E-Mail-Anlagen 81
Bericht auf Anforderung 83
Planen von Scanvorgängen auf Anforderung 85
Konsole für das Scannen auf Anforderung - Einführung 89
Die Oberfläche der Konsole für das Scannen auf Anforderung 91
Die Menüleiste 92
Das Menü „Datei“ 92
Das Menü „Ansicht“ 92
Das Menü „Scan“ 92
Das Menü „Hilfe“ 93
Die Symbolleiste 93
Das Ergebnisfenster 93
Verwenden der Konsole für das Scannen auf Anforderung 94
Verwenden der Konsole für das Scannen auf Anforderung aus dem Programmverzeichnis GroupShield für Exchange 95
Ermitteln der Versionsinformationen 98

Wechseln des Zielservers 98
Durchführen eines Scanvorgangs auf Anforderung über die Befehlszeile .99
Beispiele für Befehlszeilen 103

Kapitel 5. Benachrichtigungen und Alarmmeldungen 107
Benachrichtigungen und GroupShield für Exchange-Aktionen 108
Betreffzeilen 108
Einfügbare Ersatztexte für Benachrichtigungen 112

Kapitel 6. Serveradministration und Protokollierung 113
Administration (Registerkarte) 113
Auswählen von Administratorpostfächern für den Empfang von Benachrichtigungen 113
Auswählen einer Isolierungsmethode und eines Quarantäneortes . .116
Verhindern einer Dienstverweigerung (des Scan-Dienstes) 118
Behandlung verschlüsselter E-Mail-Nachrichten 119
Ermitteln der GroupShield Exchange-Versionsinformationen 122
Protokollieren von Virenschutz- und Systemereignissen 124
Konfigurieren der McAfee Log Manager-Ausgabe 125

Kapitel 7. Automatische Aktualisierung der .DAT-Dateien 129
Inkrementelle Aktualisierungen 130
Hinzufügen von GroupShield für Exchange-Servern, um .DAT-Dateien zu aktualisieren 130
Auswählen einer Aktualisierungsmethode 132
Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) über das Internet 133
Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) von einem entfernten Server aus 134
Zeitliche Planung der Aktualisierungen 136
Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) vom lokalen Computer aus 138

Kapitel 8. Viruswarnsystem 141
Mehrere Informationsmethoden 141
Überblick über die Warnmethoden 141
Wie viele Warnungs-Manager sind erforderlich? 143

Öffnen der Registerkarten von Warnungs-Manager 144
Konfigurieren von Warnungs-Manager 145
Anpassen von Alarmmeldungen 182

Kapitel 9. Protokollier- und Überwachungsfunktionen 189
Einführung in McAfee Log Manager 189
Die Benutzeroberfläche 190
Die Menüleiste 190
Das Menü „Datei“ 190
Das Menü "Ansicht" 191
Das Menü „Hilfe“ 192
Die Symbolleiste 192
Das Ergebnisfenster 193
Arbeiten mit Log Manager 194
Speichern der Protokolldatenbank 194
Öffnen einer archivierten Protokolldatenbank 195
Abrufen von Datensatzdetails 195
Filtern von Protokolldatensätzen 196
Hinzufügen eines neuen Filters 196
Modifizieren eines Filters 198
Löschen eines Filters 199
Hinzufügen oder Entfernen von Spalten aus der Ansicht 200
Ändern der Spaltensortierreihenfolge 201
Ermitteln der Versionsinformationen 201
Anfordern von Hilfe 202
Systemmonitor von GroupShield für Exchange 202

Kapitel 10. Quarantänemethoden 205
McAfee Quarantine Manager - Einführung 206
Die Benutzeroberfläche von Quarantine Manager 207
Die Menüleiste 207
Das Menü „Datei“ 207
Das Menü „Objekt“ 208
Das Menü „Ansicht“ 208
Das Menü „Hilfe“ 209

Die Symbolleiste 209
Das Ergebnisfenster 210
Verwenden von McAfee Quarantine Manager 211
Öffnen von Quarantine Manager 211
Speichern der Quarantäne-Datenbank 212
Öffnen einer archivierten Quarantäne-Datenbank 213
Übermitteln von Objekten, die durch neue Virusarten infiziert wurden, an Network Associates 214
Senden isolierter Objekte an andere Benutzer 214
Säubern einer infizierten Datei in der Quarantäne-Datenbank 215
Hinzufügen eines neuen Filters 215
Modifizieren eines Filters 217
Löschen eines Filters 218
Hinzufügen oder Entfernen von Spalten zur/aus der Ansicht 219
Anzeigen von Details zu einem Datensatz 220
Ermitteln der Versionsinformationen 220
Ändern der Spaltensortierreihenfolge 221
Anfordern von Hilfe 222
Das Quarantäneverzeichnis 222

Kapitel 11. Das Dienstprogramm Outbreak Manager 223

Schützen vor Virusepidemien 223
Funktionsübersicht 223
Zur Funktionsweise des Dienstprogramms Outbreak Manager 225
Installieren, Aktualisieren und Entfernen des Dienstprogramms Outbreak Manager 226
Installationsanforderungen 226
Öffnen des Dienstprogramms Outbreak Manager 227
Verwenden des Dienstprogramms Outbreak Manager 228
Übernehmen Ihrer Änderungen 229
Erstellen neuer Regeln 229
Ändern vorhandener Regeln 239
Löschen von Regeln 239
Kopieren von Regeln 240
Umbenennen von Regeln 241

Ändern der Reihenfolge von Regeln 242
Anzeigen des Regelstatus 242
Anzeigen des Ausbruchaktivität 244
Menüleiste 245
Symbolleiste 247
Ergebnisfenster 248
Filtern der Log Manager-Datenbank 248
Anzeigen von Informationen zu einem Datensatz 251
Speichern von Datensätzen 251
Entfernen von Datensätzen 252

Appendix A. Weitere Installationsszenarien 253
Installieren der Software auf einem Cluster Server 253
Entfernen der Software von einem Cluster Server 256
Installation von GroupShield für Exchange im Hintergrund 257
Systemanforderungen 257
Phase 1 - Ermitteln von Konfigurationsdetails für GroupShield für Exchange 258
Phase 2 - Ausführen der .GSE-Konfigurationsdatei 259
Installieren von GroupShield für Exchange auf mehreren Servern 260

Appendix B. McAfee-Aktualisierungsdienstprogramme 263
Aktuelle McAfee Aktualisierungsdienstprogramme 263
Die neueste Aktualisierungserweiterung: inkrementelle .DAT-Dateien 266
Was ist eine inkrementelle .DAT-Aktualisierung? 266
Funktionen der inkrementellen Aktualisierung 267
Einschränkungen der inkrementellen Aktualisierung 267
Wie funktioniert die inkrementelle Aktualisierung von .DAT-Dateien? 268
Tips 269
Häufig gestellt Fragen 270

Appendix C. McAfee-Supportdienste 273
PrimeSupport-Optionen für Firmenkunden 273
PrimeSupport KnowledgeCenter 273

PrimeSupport Connect 274
PrimeSupport Priority 274
PrimeSupport Enterprise 275
Bestellen von Corporate PrimeSupport 276
PrimeSupport-Optionen für Privatkunden 278
Bestellen von Retail PrimeSupport 279
Beratung und Schulung bei McAfee 280
Beratungsdienste durch Fachleute 280
Schnelleinstiegdienste 280
Netzwerkberatung 281
Total Education Services 281

Index 283

Vorwort

Virenschutz ist Datensicherheit

> „Die Welt änderte sich [am 26. März 1999] - oder zweifelt jemand daran? Die Welt ist anders. Melissa bewies das, und wir haben noch Glück gehabt: Die Welt wäre nahezu zerschmolzen."
>
> *—Padgett Peterson, Chief Info Security Architect, Lockheed Martin Corporation, über die „Melissa"-Virusepidemie von 1999*

Ende der Neunziger Jahre erkannten viele Informationstechnologieexperten, daß sie Methoden zur Reaktion auf neue Virusbedrohungen nicht problemlos von Methoden zur Bekämpfung absichtlicher Netzwerksicherheitsverletzungen trennen konnten. Dorothy Denning, Mitautorin des 1998 erschienenen Computersicherheitshandbuchs *Internet Besieged: Countering Cyberspace Scofflaws* (Das Internet unter Belagerung: Bekämpfung von Cyberspace-Gesetzesbrechern) stellte Virenschutzmaßnahmen ausdrücklich in eine Reihe mit anderen Netzwerksicherheitsmaßnahmen und klassifizierte sie als Verteidigung gegen bösartigen „eingeschleusten Code".

Denning begründete diesen Einschluß mit ihrer Definition von Informationssicherheit als „effiziente Verwendung von Vorrichtungen zum Schutz von Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und Nichtablehnung von Informationen und Informationsverarbeitungssystemen". Virusangriffe hatten die Datenintegrität schon immer bedroht oder geschädigt. Als sie noch ihren Artikel schrieb, hatten neuere Viren bereits damit begonnen, hochintelligente Attacken zu führen, die auf die verbleibenden Fundamente der Informationssicherheit abzielten. Dennings Klassifizierung erkannte an, daß neuere Viren nicht einfach nur Systemverwalter ärgerten oder eine relativ geringe Bedrohung darstellten, sondern in Wirklichkeit eine ernsthafte Gefahr wurden.

Obwohl Virusangriffe nicht so gezielt wie unberechtigtes Eindringen ins Netzwerk ablaufen, haben sie bereits Formen bedachter Informationskriegsführung angenommen. Einige Beispiele mögen dies verdeutlichen. Viele davon erweiterten das Repertoire der Virenschreiber um spontan kopierte Innovationen:

- W32/CIH.Spacefiller zerstörte das Flash-BIOS von infizierten Workstations, so daß diese nicht mehr gestartet werden konnten. Es überschrieb außerdem Teile der infizierten Festplatte mit sinnlosen Daten.
- XM/Compat.A überschrieb Daten in Microsoft Excel-Tabellendateien. Es verwendete moderne polymorphe Verbergungstechniken, was bedeutet, daß es bei jeder Infektion die Signaturbytes, die sein Vorhandensein anzeigten und es Virenscannern ermöglichten, es zu finden, änderte.

- W32/Ska, obwohl technisch gesehen ein Wurm, ersetzte die Winsock-Datei des infizierten Computers, so daß es sich selbst als Anlage zu Simple Mail Transfer Protocol (SMTP)-Nachrichten und Ablagen in Usenet-Newsgroups hinzufügen konnte. Diese Strategie bürgerte sich in vielen Bereichen ein.

- Remote Explorer stahl die Sicherheitsrechte eines Windows NT-Domänenadministrators und verwendete sie, um sich selbst als Windows NT-Dienst zu installieren. Es speicherte außerdem Kopien von sich selbst im Windows NT-Treiberverzeichnis und führte eine unterstützende Dynamic Link Library (.DLL)-Datei mit sich, die es ihm erlaubte, Datendateien zufällig zu verschlüsseln. Da er fast ausschließlich an einem Unternehmensstandort auftrat, spekulierten Sicherheitsexperten, daß er ein absichtlicher gezielter Angriff auf die Netzwerkintegrität der unglückseligen Firma sei.

- Back Orifice, das Produkt einer Gruppe, die sich selbst Cult of the Dead Cow (Kult der toten Kuh) nennt, behauptete, daß der Besitzer des Clientteils der Back Orifice-Anwendung unbeschränkten Remote-Zugriff auf jede Windows 95- oder Windows 98-Workstation hat, auf der der versteckte Serverteil ausgeführt wird. Dieser Zugriff—aus dem gesamten Internet heraus—ermöglichte es dem Client, Tastenanschläge abzufangen, Dateien zu öffnen, zu kopieren, zu löschen oder auszuführen, Bildschirmkopien zu übertragen und den infizierten Computer neu zu starten, abstürzen zu lassen oder herunterzufahren. Um das Maß voll zu machen, enthielten frühe Back Orifice-Versionen auf CD außerdem noch eine W32/CIH.Spacefiller-Infektion.

1999 verstärkte sich auf einen Schlag die Intensität von Virus- und Wurmangriffen und rückte sie ins öffentliche Licht. Erklären läßt sich das teilweise natürlich dadurch, daß viele der berüchtigteren Viren und Würmer das Internet voll ausnutzten und dadurch einen lange vorhergesagten Angriff starteten, indem sie E-Mail-Übertragungen, Websites, Newsgroups und andere verfügbare Kanäle mit nahezu exponentiellen Wachstumsraten überfluteten. Sie bahnten sich jetzt ihren Weg in Netzwerkumgebungen, wo sie sich rasch verbreiteten und eine teuere Spur der Verwüstung hinter sich ließen.

W97M/Melissa, das „Melissa“-Virus, rüttelte die meisten Informationstechnologieabteilungen der Unternehmen aus ihrer Unbekümmertheit, die sie auch noch angesichts neuer Virusbelastungen aufrechterhalten hatten. Als Melissa im März 1999 zuschlug, brachte es E-Mail-Server von Unternehmen in den USA und anderswo zum Erliegen. Melissa wies E-Mail-Clientprogramme an, infizierte E-Mail-Nachrichten an die ersten fünfzig Einträge im Adressbuch jedes Zielcomputers zu senden. Dies verwandelte eine einfache Makrovirusinfektion ohne echte Schadensfunktion in einen effizienten Dienstverweigerungsangriff (Denial-Of-Service) auf Mail-Server.

Melissas andere grundlegende Innovation war sein direkter Versuch, die Endbenutzerpsychologie auszunutzen: Es fälschte eine E-Mail-Nachricht von einem Absender, den der Empfänger kannte, und sendete sie mit einer Betreffzeile, die den Empfänger drängte, sowohl die Nachricht als auch die Dateianlage zu öffnen. So machte Melissa die Notwendigkeit, daß sich der Virencode selbst verbreitet, nahezu überflüssig. Endbenutzer selbst kooperierten zu seiner Verbreitung, und ihre eigenen Computer nahmen blindlings teil.

Kurz danach erschienen eine Fülle von Melissa-Varianten und -Nachäffern. Einige davon, wie z. B. W97M / Prilissa, enthielten eine zerstörerische Fracht. Im weiteren Verlauf desselben Jahres demonstrierte eine Reihe neuer Viren und Würmer neuartige oder unerwartete Methoden zum Eindringen in Netzwerke und zum Beeinträchtigen der Informationssicherheit oder führte tatsächlich ständig Angriffe aus. Beispiele waren:

- W32 / ExploreZip.worm und seine Varianten, die einige von Melissas Techniken verwendeten, um sich - anfangs per E-Mail - zu verbreiten. Nachdem ExploreZip einen Hostcomputer erfolgreich infiziert hatte, suchte es nach ungesicherten freigegebenen Netzwerkverzeichnissen und kopierte sich unbemerkt über das ganze Netzwerk. Es trug zerstörerischen Code mit sich, der verschiedene Windows-Systemdateien und Microsoft Office-Dokumente löschte und durch nicht mehr wiederherstellbare Dateien von 0-Byte-Größe ersetzte.

- W32 / Pretty.worm, der auf Melissa noch eines draufsetzte, indem er sich selbst an *jeden* Eintrag im MAPI-Adressbuch des infizierten Computers sendete. Er verband sich auch mit einem Internet Relay Chat (IRC)-Server, nahm an einem bestimmten IRC-Kanal teil und öffnete dann einen Pfad zum Empfang von Befehlen über die IRC-Verbindung. Dies ermöglichte es Teilnehmern im Kanal im Prinzip, Informationen von dem infizierten Computer abzusaugen: Name und Besitzer des Computers, Benutzername und -kennwort des DFÜ-Netzwerks und Pfad zum Systemstammverzeichnis.

- W32 / FunLove.4099, das unter anderem ActiveX .OCX-Dateien infizierte. Dies bedeutete, daß es auf Web-Seiten mit ActiveX-Inhalt lauern und beim Herunterladen von Seiten auf ihre Festplatte Systeme mit niedrigen oder ausgeschalteten Browser-Sicherheitseinstellungen infizieren konnte. Wenn ein Windows NT-Computerbenutzer sich bei einem System mit Administratorrechten angemeldet hatte, veränderte das infizierende Virus zwei kritische Systemdateien, die *allen* Benutzern im Netzwerk - *einschließlich* dem Virus - Administratorrechte für alle Dateien auf dem Zielcomputer gaben. Es verbreitete sich im Netzwerk weiter, indem es sich selbst an Dateien mit den Erweiterungen .SCR, .OCX und .EXE anhängte.

- VBS / Bubbleboy trat den Beweis an, daß es möglich ist, daß ein Virus Zielcomputer direkt aus E-Mail-Nachrichten infizieren kann, ohne sich über Nachrichtenanlagen verbreiten zu müssen. Es umging den Desktop-Virenschutz komplett, zumindest zu Beginn. Seine Kombination

aus HTML und VBScript nützte vorhandene Schwachstellen in internetfähigen Mail-Systemen aus; sein Autor verließ sich auf dieselbe Endbenutzerpsychologie, die Melissa so erfolgreich machte.

Die andere bemerkenswerte Entwicklung in diesem Jahr war das Ausmaß, in dem Virenschreiber die Techniken ihrer Kollegen kopierten, verschmolzen und erweiterten. Diese gegenseitige Befruchtung gab es auch schon zuvor, doch die Geschwindigkeit, mit der sie erfolgte, und die gestiegene Komplexität der Tools und Techniken, die in diesem Zeitraum verfügbar wurden, bereiteten einen äußerst fruchtbaren Boden für die nervös erwartete überreiche Ernte komplizierter Viren.

Informationssicherheit als Geschäftsnotwendigkeit

Zufall oder nicht, diese unheilvoll schöpferischen neuen Virenangriffe und schnellen Verbreitungsmethoden traten auf, als immer mehr Unternehmen den Schritt zu internetbasierten Informationssystemen und E-Commerce-Operationen unternahmen. Die Bequemlichkeit und Effizienz, die das Internet den Unternehmen brachte, sparte Geld und erhöhte die Profite. Dies machte vermutlich auch dieselben Unternehmen zu attraktiven Zielen für Lausbuben, den Hacker-Untergrund und alle, die darauf bedacht sind, ihre favorisierten Ziele anzugreifen.

Bis dahin resultierten die wesentlichen Kosten eines Virusangriffs aus Zeit und Geld, die zum Bekämpfen einer Infektion und zum Wiederherstellen der Funktionsfähigkeit des Computersystems erforderlich waren. Zu diesen Kosten kommen durch die neuartigen Virusangriffe jetzt noch die Schäden durch Produktivitätverlust, Netzwerk- und Serverausfall, Dienstverweigerung für E-Mail und andere geschäftskritische Tools, Bekanntwerden - und möglicherweise weiträumige Verbreitung - von vertraulichen Informationen und anderen Übeln.

Letzten Endes wird der einzige Unterschied zwischen einem von Hackern durchgeführten Sicherheitseinbruch in ein Netzwerk und einem Sicherheitseinbruch, der durch einen Virusangriff hervorgerufen wird, in Absicht und Methode und nicht im Ergebnis liegen. Schon haben wieder neue Angriffe die Grundfeste internetbasierender Unternehmen erschüttert. Viele davon benötigen eine 24-stündige Verfügbarkeit ihrer Netzwerke und E-Mail, hohe Datenintegrität, vertrauliche Kundenlisten, sichere Kreditkartendaten und Kaufnachweise, zuverlässige Kommunikation und Hunderte von anderen computergestützten Transaktionsdetails. Die Kosten durch diese Virenangriffe wirken sich in der digitalen Ökonomie unmittelbar auf das Geschäftsergebnis aus.

Aus diesem Grund bedeutet ein Schutz des Geschäftsergebnisses die Implementierung einer Gesamtlösung für Informations- und Netzwerksicherheit, eine Lösung, zu der umfassender Virenschutz gehört. Es reicht nicht, sich nur auf Desktop-basierten Virenschutz oder willkürliche oder spontane Sicherheitsmaßnahmen zu verlassen. Die beste Verteidigung erfordert es, alle möglichen Punkte - von der Firewall und dem Gateway bis zur einzelnen Workstation - über die Viren in Ihr Netzwerk eindringen oder es angreifen können, zu versiegeln und die Virenschutzwächter an diesen Punkten immer auf dem neuesten Stand zu halten.

Teil dieser Lösung ist der Einsatz der McAfee Active Virus Defense*-Software-Produktfamilie, die eine umfassende Multiplattformreihe von Verteidigungsperipherie für Ihr Netzwerk bietet. Sie können diese Sicherheit auch mit der McAfee Active Security-Produktfamilie ausbauen, die Ihnen die Überwachung Ihres Netzwerks gegen Eindringlinge, die Überwachung des tatsächlichen Netzwerkpaketverkehrs und das Verschlüsseln von E-Mail- und Netzwerkübertragungen ermöglicht. Doch selbst bei installierter Virenschutz- und Sicherheitssoftware finden neue und bisher unbekannte Viren ihren Weg in Ihr Netzwerk. Und hier kommt die andere Seite der Gleichung ins Spiel: eine gründliche, leicht zu befolgende Virenschutz-Sicherheitsrichtlinie und praktische Anweisungen für Ihr Unternehmen. Nur so kann letztendlich ein Virusangriff gestoppt werden, bevor eine Virusepidemie daraus wird.

Active Virus Defense-Sicherheitsperipherie

Die McAfee Active Virus Defense-Produktfamilie gibt es aus einem einfachen Grund: für das moderne, automatisierte Unternehmen gibt es niemals zu viel Virenschutz. Zwar mag es auf den ersten Blick überflüssig erscheinen, alle Desktop-Computer, Datei- und Netzwerkserver, Gateways, E-Mail-Server und Firewalls zu schützen, doch erfüllt jeder dieser Knoten in Ihrem Netzwerk eine andere Funktion. Ein Virenschutzscanner, der dazu bestimmt ist, eine Workstation virenfrei zu halten, kann zum Beispiel keine Viren abfangen, die E-Mail-Server überfluten und effektiv arbeitsunfähig machen. Sie würden wohl auch kaum einen Dateiserver damit beauftragen, ständig seine Client-Arbeitsstationen zu scannen - dies würde zu sehr zu Lasten der Netzwerkbandbreite gehen.

Genauer gesagt, bedeuten die speziellen Funktionen jedes Knotens, daß Viren sie auf verschiedene Arten infizieren, was optimierte Virenschutz-Lösungen verlangt. Viren und anderer bösartige Code kann aus einer Vielzahl von Quellen in Ihr Netzwerk gelangen: Disketten und CDs, E-Mail-Anlagen, heruntergeladene Dateien, Internetsites usw. Diese unvorhersehbaren Eintrittspunkte bedeuten, daß infizierende Agents durch die Ritzen eines unvollständigen Virenschutzpanzers schlüpfen können.

Desktop-Arbeitsstationen zum Beispiel können Viren auf vielen Wegen ausbreiten: über Disketten, durch Herunterladen aus dem Internet, durch Zuordnen freigegebener Serververzeichnisse oder Festplatten anderer Arbeitsstationen. E-Mail-Server verwenden im Gegensatz dazu selten Disketten oder Netzlaufwerke; das Melissa-Virus zeigte jedoch, daß sie gegenüber Infektionen durch E-Mails ziemlich verwundbar sind, auch wenn sie den Viruscode nicht selbst ausführen.

Auf Ihrem Microsoft Exchange-Server

Die McAfee Active Virus Defense-Produktreihe bietet für jeden Schwachpunkt eine spezielle und optimierte Virenschutzanwendung. Auf Ihrem Microsoft Exchange-Server ist dies das McAfee-Virenschutzprodukt GroupShield für Exchange.

Die GroupShield-Software schützt einige der anfälligsten Viruseintrittspunkte durch eine miteinander verzahnte Palette von Scannern, Dienstprogrammen und unterstützenden Dateien, die Microsoft Exchange-Postfächer abschirmen können. GroupShield für Exchange scannt E-Mail-Nachrichten und -Anlagen in Postfächern und öffentlichen Ordnern. Dies kann einige Melissa-artige Infektionen sowie Infektionen durch die nächste Generation von VBS/Bubbleboy vermeiden.

GroupShield-Software kombiniert diese leistungsfähigen Scanfähigkeiten mit leistungsfähigen Warn-, Aktualisierungs- und Verwaltungstools. Dazu gehören:

- Warnungs-Manager-Konfiguration. GroupShield-Software enthält ein Konfigurationsdienstprogramm, mit dem Sie Alarmmeldungen direkt an Warnungs-Manager-Server in ihrem Netzwerk, an ein freigegebenes Verzeichnis für zentrale Warnungen oder an eine DMI (Desktop Management Interface)-Verwaltungsanwendung senden können. Weitere Warnmethoden sind lokale benutzerdefinierte Meldungen und Signaltöne, Erkennungsalarme und Reaktionsoptionen sowie E-Mail-Warnnachrichten.
- AutoUpdate-Dienstprogramme der nächsten Generation. AutoUpdate v4.5 bietet eine umfassende und transparente Unterstützung für die neuen inkrementellen .DAT-Dateiupdates. Diese sparen Zeit und Netzwerkbandbreite, indem sie nur Virusdefinitionen hinzufügen, die auf Ihrem System noch nicht installiert sind.
- Outbreak Manager. GroupShield für Exchange enthält das McAfee-Dienstprogramm Outbreak Manager, das Virusausbrüche automatisch verwaltet oder Administratoren beim Aufräumen nach einem Virenangriff unterstützt. Dieses Dienstprogramm hilft beim Minimieren der Unterbrechung, die ein über E-Mail verbreitetes Virus in der gesamten Organisation verursacht, indem es rasch Maßnahmen ergreift, bevor die Verbreitung zu weit gediehen ist.

Insgesamt bildet die Active Virus Defense-Reihe einen dichten Gürtel von Virenschutz-Sicherheitsperipherie um Ihr Netzwerk, das Sie sowohl gegen externe als auch interne Infektionsquellen schützt. Wenn diese Peripherie richtig konfiguriert und in Verbindung mit einer klaren unternehmensweiten Virenschutz-Sicherheitspolitik implementiert ist, bietet sie in der Tat nützliche Redundanz. Ihr Hauptvorteil liegt jedoch in ihrer Fähigkeit, Viren zu stoppen, wenn sie in Ihr Netzwerk *eindringen*, d. h. nicht erst mit Verzögerung oder zufällig entdeckt werden. Bei frühzeitiger Erkennung werden Infektionen eingedämmt und bei der Virusbeseitigung Kosten eingespart. In vielen Fällen kann auch verhindert werden, daß zerstörerischer Viruscode ausgelöst wird.

McAfee-Virenschutzforschung

Auch die beste Virenschutzsoftware ist nur so gut wie ihr letztes Update. Da jeden Monat 200 bis 300 Viren und Varianten erscheinen, können die .DAT-Dateien, mit deren Hilfe McAfee-Software Viren erkennen und entfernen kann, schnell veralten. Werden diese Dateien der ursprünglichen Software nicht aktualisiert, so riskieren Sie Infektionen durch neu auftauchende Viren. McAfee hat jedoch in seinem AVERT*-Team (Anti-Virus Emergency Response Team) die weltweit meisten und erfahrensten Virenschutzforscher versammelt. Diese erstklassige Virenschutzforschungsorganisation deckt die ganze Welt ab und arbeitet rund um die Uhr. So ist sichergestellt, daß Sie die zum Bekämpfen neuer Viren benötigten Dateien erhalten, sobald—oder oft sogar bevor—Sie sie brauchen. Sie können von vielen unmittelbaren Ergebnissen dieser Forschung profitieren, wenn Sie die AVERT-Forschungssite auf der Network Associates-Website besuchen:

http://www.nai.com/asp_set/anti_virus/introduction/default.asp

Wenden Sie sich an Ihren McAfee-Vertreter, oder besuchen Sie die McAfee-Website, um herauszufinden, wie Sie die Leistungsfähigkeit der Active Virus Defense-Sicherheitslösung bei sich entfalten können:

http://www.mcafeeb2b.com/

So nehmen Sie Kontakt zu McAfee und Network Associates auf

Kundendienst

Am 1. Dezember 1997 fusionierte McAfee Associates mit Network General Corporation, Pretty Good Privacy, Inc., und Helix Software, Inc. zu Network Associates, Inc. Diese gemeinsame Firma erwarb später Dr Solomon's Software, Trusted Information Systems, Magic Solutions und CyberMedia, Inc.

Aus einer im Januar 2000 durchgeführten Firmenreorganisation gingen vier unabhängige Geschäftbereiche hervor, die sich jeweils auf eine bestimmte Produktlinie spezialisieren. Die neuen Geschäftsbereiche lauten:

- **Magic Solutions**. Diese Abteilung betreut die Helpdesk-Produktlinie "Total Service Desk" sowie andere Produkte der gleichen Kategorie.
- **McAfee**. Diese Abteilung stellt die Produktfamilie "Active Virus Defense" und andere Antivirus-Softwarelösungen für Firmen- und Privatkunden bereit.
- **PGP Security**. Diese Abteilung ist zuständig für preisgekrönte Verschlüsselungs- und Datensicherheitslösungen einschließlich der PGP-basierten Produkte für Datensicherheit und Verschlüsselung, der „Gauntlet“-Firewall-Produkte, der „WebShield E-ppliance“-Hardwaresysteme sowie der Produkte „CyberCop Scanner“ und „CyberCop Monitor“.
- **Sniffer Technologies**. Diese Abteilung betreut „Sniffer“, das führende Dienstprogramm zur Analyse, Überwachung und Auswertung von Netzwerkaktivitäten, sowie andere Softwareprodukte der gleichen Kategorie.

Network Associates ist weiterhin zuständig für Vermarktung und Support der Produktlinien aller neuen unabhängigen Geschäftbereiche. Alle Fragen, Kommentare oder Wünsche hinsichtlich der von Ihnen erworbenen Software, der Registrierung oder ähnlicher Themen können Sie an die Kundendienstabteilung von Network Associates unter der folgenden Adresse richten:

Network Associates Deutschland GmbH
Ohmstraße 1
D-85716 Unterschleißheim
Deutschland

Weitere Kontaktinformationen für Firmenkunden:

Telefon: (972) 308-9960

Fax: +1 972-619-7485 (24-Stunden-Service, Gruppe-III-Fax)

E-Mail: services_corporate_division@nai.com

Web: http://www.nai.com

Weitere Kontaktinformationen für Privatkunden:

Telefon: (972) 308-9960

Fax: +1 972-619-7485 (24-Stunden-Service, Gruppe-III-Fax)

E-Mail: cust_care@nai.com

Web: http://www.mcafee.com/

Technischer Support

Wie von vielen Seiten bestätigt wird, steht bei McAfee und Network Associates die Kundenzufriedenheit an oberster Stelle. Die beiden Firmen setzen diese Tradition fort, indem sie ihre Sites im World Wide Web zu wertvollen Ressourcen für Fragen an den technischen Support gemacht haben. McAfee empfiehlt Ihnen, sie zu Ihrer ersten Quelle für Antworten auf häufig gestellte Fragen, für Updates von McAfee-Software bzw. Network Associates-Software und für den Zugriff auf News und -Virusinformationen zu machen.

World Wide Web	http://www.nai.com/asp_set/services/technical_support/tech_intro.asp

Wenn Sie das Gesuchte nicht finden oder keinen Webzugriff haben, probieren Sie einen unserer automatischen Dienste aus.

Internet	techsupport@mcafee.com
CompuServe	GO NAI
America Online (AOL)	Stichwort MCAFEE

Wenn Ihnen die automatischen Dienste nicht die benötigten Antworten liefern, können Sie sich von Montag bis Freitag zwischen 8 und 20 Uhr (amerikanische Zentralzeit) unter den folgenden Telefonnummern an Network Associates wenden, um sich über die technischen Supportpläne von Network Associates zu informieren.

Für Kunden mit Unternehmenslizenz:

Telefon	(972) 308-9960
Fax	(972) 619-7845

Für Kunden mit Einzellizenz:

Telefon	(972) 855-7044
Fax	(972) 619-7845

Dieses Handbuch enthält eine Übersicht über die PrimeSupport-Pläne, die für McAfee-Kunden verfügbar sind. Weitere Informationen finden Sie in Anhang C, „McAfee-Supportdienste“

Um die benötigten Antworten rasch und effizient zu finden, benötigen die Mitarbeiter des technischen Supports von Network Associates einige Informationen über Ihren Computer und Ihre Software. Nehmen Sie bitte die folgenden Informationen in Ihren Schriftverkehr auf:

- Produktname und Versionsnummer
- Computermarke und -modell
- Alle weiteren an den Computer angeschlossenen Hardware- oder Peripheriegeräte
- Betriebssystemtyp und Versionsnummer
- Netzwerktyp und -version (falls zutreffend)
- Inhalt Ihrer AUTOEXEC.BAT- und CONFIG.SYS-Dateien und des LOGIN-Skripts des Systems
- Spezifische Schritte zur Reproduktion des Problems

Support für Herunterladen

Informationen, die Ihnen die Orientierung innerhalb der Websites oder FTP-Sites von Network Associates oder McAfee und den Download von Dateien erleichtern, können Sie über folgende Rufnummern erhalten:

Firmenkunden	(801) 492-2650
Privatkunden	(801) 492-2600

Network Associates-Schulung

Informationen über Termine für firmeninterne Schulungen von McAfee- oder Network Associates-Produkten erhalten Sie beim Network Associates-Kundendienst unter dieser Rufnummer: (972) 308-9960.

Kommentare und Feedback

McAfee schätzt Ihre Kommentare und behält sich das Recht vor, jede von Ihnen bereitgestellte Information nach eigenem Gutdünken zu verwenden, ohne damit irgendwelche Verpflichtungen einzugehen. Senden Sie bitte ihre Kommentare zur McAfee-Virenschutz-Produktdokumentation an: Network Associates Deutschland GmbH, Ohmstraße 1, D-85716 Unterschleißheim Sie können Kommentare auch per Fax an diese Nummer senden: (503) 466-9671. Oder senden Sie eine E-Mail an tvd_documentation@nai.com.

Melden neuer Posten für Virenschutzdatendateien

McAfee Virenschutzsoftware bietet Ihnen die besten verfügbaren Erkennungs- und Entfernungsfähigkeiten samt einem erweiterten heuristischen Scannen, das neue und unbenannte Viren entdecken kann, sobald sie auftauchen. Gelegentlich kann jedoch auf Ihrem System ein völlig neuer Virentyp auftreten, der keine Variante eines älteren Typs ist und der Erkennung entgeht.

Da die Forscher von McAfee immer bestrebt sind, Ihnen für den Schutz Ihrer Systeme jeweils effektive und nach dem neuesten Stand der Technik arbeitende Werkzeuge zur Hand zu geben, sind wir sehr daran interessiert, daß Sie uns über alle neuen Java-Klassen, ActiveX-Steuerelemente, zweifelhaften Websites oder Viren berichten, die die von Ihnen verwendete Software nicht zu entdecken vermag. Beachten Sie bitte, daß McAfee sich das Recht vorbehält, jede von Ihnen bereitgestellte Information nach Gutdünken zu verwerten, ohne daß sich daraus irgendwelche Verpflichtungen ableiten lassen. Senden Sie Ihre Fragen oder Beispiele von Viren an:

virus_research@nai.com	Verwenden Sie diese Adresse, um Fragen oder Beispiele von Viren zu unseren Niederlassungen in Nord- bzw. Südamerika zu senden
vsample@nai.com	Verwenden Sie diese Adresse, wenn Sie Fragen oder Virusbeispiele, die mit Dr Solomon's Anti-Virus Toolkit* Software gesammelt wurden, an unsere Büros in Großbritannien senden möchten

Um Objekte an das europäische oder südafrikanische McAfee-Forschungbüro zu melden, verwenden Sie bitte diese E-Mail Adressen:

virus_research_europe@nai.com	Verwenden Sie diese Adresse, um Fragen oder Beispiele von Viren zu unserer Niederlassung in Westeuropa zu senden
virus_research_sa@nai.com	Verwenden Sie diese Adresse, um Fragen oder Beispiele von Viren an unsere Niederlassung in Südafrika zu senden
virus_research_de@nai.com	Verwenden Sie diese Adresse, um Fragen oder Beispiele von Viren, die mit Dr Solomons Anti-Virus-Toolkit gefunden wurden, zu unserer Niederlassung in Deutschland zu senden

Wenn Sie Objekte dem McAfee-Forschungsbüro für Asien-Pazifik oder dem Büro in Japan melden möchten, verwenden Sie eine der folgenden E-Mail-Adressen:

virus_research_japan@nai.com	Verwenden Sie diese Adresse, um Fragen oder Beispiele von Viren zu unseren Niederlassungen in Japan und Ostasien zu senden
virus_research_apac@nai.com	Verwenden Sie diese Adresse, wenn Sie Fragen oder Virusbeispiele an unsere Büros in Australien und Südostasien senden möchten

Internationale Kontaktinformationen

Um Kontakt mit Network Associates außerhalb der USA aufzunehmen, verwenden Sie bitte die unten genannten Adressen und Telefonnummern.

Network Associates
Australien

Level 1, 500 Pacific Highway
St. Leonards, NSW
Sydney, Australia 2065
Telefon: 61-2-8425-4200
Fax: 61-2-9439-5166

Network Associates
Österreich

Pulvermuehlstrasse 17
A-4040 Linz
Österreich
Telefon: 43-732-757-244
Fax: 43-732-757-244-20

Network Associates
Belgien

BDC Heyzel Esplanade, boîte 43
1020 Bruxelles
Belgien
Telefon: 0032-2 478.10.29
Fax: 0032-2 478.66.21

Network Associates
do Brasil

Rua Geraldo Flausino Gomez 78
Cj. - 51 Brooklin Novo - São Paulo
SP - 04575-060 - Brasil
Telefon: (55 11) 5505 1009
Fax: (55 11) 5505 1006

Network Associates Kanada

139 Main Street, Suite 201
Unionville, Ontario
Kanada L3R 2G6
Telefon: (905) 479-4189
Fax: (905) 479-4540

Network Associates Volksrepublik China

Room 913, Tower B
Full Link Plaza
No. 18 Chao Yang Men Wai Avenue
Beijing
Volksrepublik China 100020
Telefon: 86-10-6538-3399
Fax: 86-10-6588-5601

Network Associates Denmark

Lautruphoej 1-3
2750 Ballerup
Dänemark
Telefon: 45 70 277 277
Fax: 45 44 209 910

NA Network Associates Oy

Mikonkatu 9, 5. krs.
00100 Helsinki
Finnland
Telefon: 358 9 5270 70
Fax: 358 9 5270 7100

Network Associates France S.A.

50 rue de Londres
75008 Paris
Frankreich
Telefon: 33 1 44 908 737
Fax: 33 1 45 227 554

Network Associates Deutschland GmbH

Ohmstraße 1
D-85716 Unterschleißheim
Deutschland
Telefon: 49 (0)89/3707-0
Fax: 49 (0)89/3707-1199

Network Associates Hong Kong

14th Floor, Plaza 2000
2-4 Russel Street
Causeway Bay
Hongkong
Telefon: 852-2892-9500
Fax: 852-2832-9530

Network Associates Srl

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italien
Telefon: 39 02 92 65 01
Fax: 39 02 92 14 16 44

Network Associates Japan, Inc.

Shibuya Mark City West 20F
1-12-1 Dougenzaka, Shibuya-ku
Tokyo 150-0043, Japan
Telefon: 81 3 5428 1100
Fax: 81 3 5428 1480

Network Associates Latin America

1200 S. Pine Island Road, Suite 375
Plantation, Florida 33324
USA
Telefon: (954) 452-1731
Fax: (954) 236-8031

Network Associates de Mexico

Andres Bello No. 10, 4 Piso
4th Floor
Col. Polanco
Mexico D.F. 11560
Telefon: (525) 282-9180
Fax: (525) 282-9183

Network Associates International B.V.

Gatwickstraat 25
1043 GL Amsterdam
Niederlande
Telefon: 31 20 586 6100
Fax: 31 20 586 6101

Network Associates Portugal

Av. da Liberdade, 114
1269-046 Lisboa
Portugal
Telefon: 351 1 340 4543
Fax: 351 1 340 4575

Net Tools Network Associates Südafrika

Hawthorne House
St. Andrews Business Park
Meadowbrook Lane
Bryanston, Johannesburg
Südafrika 2021
Telefon: 27 11 700-8200
Fax: 27 11 706-1569

Network Associates Südostasien

78 Shenton Way
#29-02
Singapur 079120
Telefon: 65-222-7555
Fax: 65-220-7255

Network Associates Spanien

Orense 4, 4ª Planta.
Edificio Trieste
28020 Madrid, Spanien
Telefon: 34 9141 88 500
Fax: 34 9155 61 404

Network Associates Schweden

Datavägen 3A
Box 596
S-175 26 Järfälla
Schweden
Telefon: 46 (0) 8 580 88 400
Fax: 46 (0) 8 580 88 405

Network Associates AG

Baeulerwisenstrasse 3
8152 Glattbrugg
Schweiz
Telefon: 0041 1 808 99 66
Fax: 0041 1 808 99 77

Network Associates Taiwan

Suite 6, 11F, No. 188, Sec. 5
Nan King E. Rd.
Taipei, Taiwan
Telefon: 886-2-27-474-8800
Fax: 886-2-27-635-5864

Network Associates International Ltd.

227 Bath Road
Slough, Berkshire
SL1 5PP
Großbritannien
Telefon: 44 (0)1753 217 500
Fax: 44 (0)1753 217 520

Willkommen bei GroupShield für Exchange 1

McAfee GroupShield® für Exchange v4.5 ist eine leistungsfähige Virenschutzlösung für Microsoft Exchange-Server. GroupShield für Exchange ist ein wesentliches Element eines umfangreichen Programms für Netzwerksicherheit, das eine Vielzahl von Sicherheitsmaßnahmen beinhaltet z. B. bietet es regelmäßige Sicherungen, umfassenden Kennwortschutz, Schulung und erhöht das Bewußtsein für Virusgefahren.

GroupShield für Exchange wird nahtlos in Ihre Microsoft Exchange-Software integriert. Sobald GroupShield für Exchange installiert wurde, schützt die Software das Microsoft Exchange-Netzwerk durch:

- Kontinuierliches Überwachen der Microsoft Exchange-Server und Schützen der Server vor Viren und Trojanischen Pferden, die über E-Mail-Nachrichten eingeschleust werden. GroupShield für Exchange nutzt die Microsoft VirusScan API (Application Programming Interface), um Viren zu entdecken und unschädlich zu machen, die versuchen, in das System einzudringen oder es zu durchlaufen.
- Scannen der Postfächer und Öffentlichen Ordner auf dem Microsoft Exchange-Server. Dies unterstützt Sie dabei, Ihre Umgebung virenfrei zu halten. GroupShield für Exchange kann eine infizierte E-Mail-Nachricht oder Anlage abfangen, säubern und protokollieren, bevor sie sich verbreitet.

Mit GroupShield für Exchange können Sie Scanvorgänge einwandfrei steuern. Sie können einen Scanvorgang jederzeit oder entsprechend einem Zeitplan initiieren, die Postfächer, Öffentlichen Ordner und Dateien angeben, die gescannt werden sollen, auswählen, wie auf Virusinfektionen reagiert werden soll und vollständige Berichte zu den Aktionen anzeigen, die GroupShield für Exchange unternommen hat.

Wenn ein Virus entdeckt wurde, können Sie reagieren, indem Sie das Virus entfernen oder indem Sie die infizierten E-Mail-Nachrichten oder Anlagen in einen Quarantäneordner verschieben (isolieren), wo sie bis zur weiteren Behandlung verbleiben. GroupShield für Exchange kann Sie und andere Administratoren über Virusinfektionen benachrichtigen und automatische Aktualisierungen der Virusdefinitionsdateien (.DAT -Dateien) vornehmen.

Der Lieferumfang GroupShield für Exchange

GroupShield für Exchange umfaßt mehrere Komponenten, die dazu beitragen, Ihre Microsoft Exchange-Server gegen Viren und andere schädliche Software zu schützen:

- Die Serververwaltungskonsole GroupShield-Eigenschaften

  Verwenden Sie die Konsole zum Konfigurieren und Verwalten GroupShield für Exchange zum Schutz Ihrer Mail-Server vor Virusinfektionen.

- GroupShield für Exchange-Konsole für das Scannen auf Anforderung

  Die GroupShield für Exchange-Konsole für das Scannen auf Anforderung zeigt das Fortschreiten und statistische Informationen zu einem Scanvorgang auf Anforderung an.

- GroupShield für Exchange-Systemmonitor

  GroupShield für Exchange-Systemmonitor überwacht kontinuierlich die GroupShield für Exchange-Virenschutzaktivitäten und sendet die Ergebnisse an Microsoft Windows NT Systemmonitor.

- McAfee Log Manager

  GroupShield für Exchange Log Manager stellt Ereignisinformationen zu den GroupShield für Exchange-Virenschutzaktivitäten bereit. Mit Log Manager können Sie Berichte und Archivprotokolle erstellen.

- McAfee Quarantine Manager

  GroupShield für Exchange kann angewiesen werden, infizierte Nachrichten oder Anlagen in eine Quarantänedatenbank oder in ein Verzeichnis Ihrer Wahl zu verschieben, wo sie bis zur weiteren Behandlung verbleiben.

- McAfee Warnungs-Manager

  Der McAfee Warnungs-Manager stellt Warnoptionen bereit, die Sie und andere Benutzer warnen, wenn Virusangriffe vorliegen. Die Warnungen können abhängig von Ihrer Arbeitsumgebung einzeln oder in Kombination eingesetzt werden.

- McAfee Outbreak Manager

  Outbreak Manager überwacht aktiv den E-Mail-Verkehr, um rechtzeitig warnen zu können, wenn eine Virusepidemie vorliegt. Das Dienstprogramm sucht nach mehreren Versionen desgleichen Virus, identischen Anlagen oder es überwacht E-Mail-Nachrichten über einen von Ihnen festgelegten Zeitraum. Wenn das Outbreak Manager-Dienstprogramm ungewöhnliches Verhalten identifiziert, reagiert es sofort gemäß den von Ihnen festgelegten Regeln.

In der Dokumentation von GroupShield für Exchange ist folgendes enthalten:

- Das vorliegende Administratorhandbuch

  Das Administratorhandbuch beschreibt ausführlich, wie GroupShield für Exchange installiert und verwendet wird. Außerdem enthält es Hintergrundinformationen sowie Informationen zu erweiterten Konfigurations- und Bereitstellungsoptionen. Sie können das Administratorhandbuch direkt von der McAfee Total Virus Defense* (TVD)- oder McAfee Active Virus Defense* (AVD)-CD-ROM öffnen und im Adobe Acrobat-.PDF-Format auf der Festplatte installieren. Adobe Acrobat-.PDF-Dateien sind flexible Onlinedokumente, die zur einfachen Navigation und zum einfachen Finden von Informationen Hyperlinks, Inhaltsverzeichnisse und andere Hilfen enthalten.

  Kopien der Produktdokumentation sind auch auf der Network Associates-Website unter dieser Adresse verfügbar:

  http://www.nai.com/asp_set/download/upgrade/find.asp

  Eine kostenlose Kopie der neuesten Version von Adobe Acrobat Reader ist ebenfalls im Lieferumfang der McAfee-Installations-CD enthalten. Außerdem kann die aktuelle englische Version von der Network Associates-Website unter der folgenden Adresse gedownloadet werden:

  http://www.nai.com/asp_set/download/upgrade/find.asp

- Online-Hilfedateien

  Die Serververwaltungskonsole GroupShield-Eigenschaften wird mit einem Online-Hilfesystem ausgeliefert, das schnellen Zugriff auf Informationen und Anweisungen zur Verwendung der Features und Funktionen von GroupShield für Exchange ermöglicht. Um die Hilfedatei zu öffnen, klicken Sie auf einer beliebigen GroupShield für Exchange-Registerkarte auf **Hilfe**. Für die GroupShield für Exchange-Konsole für das Scannen auf Anforderung und die McAfee Outbreak Manager-Funktionen gibt es eigene spezielle Hilfesysteme und sowohl für Quarantine Manager- als auch für LogManager-Funktionen steht kontextbezogene Hilfe zur Verfügung.

- README.RTF

  Die Datei README.RTF enthält Last-Minute-Ergänzungen oder -Änderungen zur Dokumentation von GroupShield für Exchange, listet bekannte Verhaltensweisen oder andere Probleme der Produktversion auf und beschreibt neue Produktmerkmale. Die Datei README.RTF von GroupShield für Exchange finden Sie im Stammverzeichnis des Programmordners von GroupShield für Exchange oder auf der McAfee-Installations-CD. Sie können die Datei in Microsoft Windows WordPad oder in nahezu jedem Textverarbeitungsprogramm öffnen und drucken.

- LICENSE.RTF

  Diese Datei wird im Microsoft Windows Installer angezeigt. Sie enthält die Lizenzbestimmungen und Bedingungen für den Einsatz von GroupShield für Exchange. Lesen Sie diese sorgfältig durch. Durch Installieren von GroupShield für Exchange stimmen Sie diesen Bestimmungen zu.

Wichtigste Features von GroupShield für Exchange

GroupShield für Exchange v4.5 beinhaltet die folgenden Hauptfunktionen:

- Verwendet die Microsoft Virus Scan-API.
- Installiert und verwaltet seine Komponenten unter Verwendung der neuen Microsoft Windows Installer-Technologie.
- Aktualisiert die McAfee- .DAT -Dateien (Virusdefinitionsdateien) unter Verwendung der verbesserten AutoUpdate-Technologie automatisch.
- Sucht mit Hilfe von Scanvorgängen auf Anforderung nach Viren in VBScript, die im Nachrichtentext von E-Mails eingebettet sind.
- Schützt Ihren Microsoft Exchange-Server vor Dienstverweigerungsattacken.
- Identifiziert, isoliert oder löscht Anlagen, die eingebettete Makros enthalten oder löscht die Makros selbst aus den Anlagen.
- Blockiert von Ihnen ausgewählte Anlagentypen während der Ausführung von Scanvorgängen bei Zugriff.
- Scannt nur die Nachrichten oder Anlagen, die sich seit dem letzten Scanvorgang auf Anforderung geändert haben.
- Beendet alle Formen von bösartigem Code, darunter Viren, Trojanische Pferde, feindliche Applets und andere codebasierte Sicherheitsgefährdungen für Ihr System.
- Steuert geschützte Microsoft Exchange-Server von einem beliebigen Microsoft Windows NT-Server oder einer Arbeitsstation, auf dem / der das Microsoft Exchange-Administratorprogramm ausgeführt wird.
- Bietet maximalen Schutz bei minimalen Auswirkungen auf Ihr Netzwerk durch geplante Scanvorgänge auf Anforderung und bei Zugriff.
- Verwendet zum Konfigurieren seiner Scanoptionen die in Microsoft Exchange integrierte Verwaltungsumgebung.
- Stellt Protokoll- und Quarantänedatenbank für Informationen und Analysen bereit.
- Benachrichtigt auf Wunsch einen Administrator, geplante Empfänger und Absender, wenn bei einem Scanvorgang auf Anforderung ein Virus entdeckt wird.

Erste Schritte 2

Bevor Sie beginnen

McAfee empfiehlt Ihnen, dieses Kapitel sorgfältig durchzulesen, bevor Sie GroupShield für Exchange installieren. Es enthält wichtige Informationen, wie Sie GroupShield für Exchange einfach und erfolgreich installieren können.

Lieferumfang von GroupShield für Exchange

McAfee vertreibt GroupShield für Exchange auf zweierlei Arten: als Archivdatei, die Sie von der Network Associates-Website oder anderen Onlinediensten herunterladen können, oder auf den CD-ROMs der Produkte „McAfee Total Virus Defense“ (TVD) oder „McAfee Active Virus Defense“ (AVD).

Sobald Sie ein Programmarchiv von GroupShield für Exchange heruntergeladen oder Ihre McAfee-Installations-CD in Ihr CD-ROM-Laufwerk eingelegt haben, können Sie mit den Installationsschritten ab Seite 34 fortfahren.

Rechte and Berechtigungen

Zur Installation und Verwaltung des Programms GroupShield für Exchange müssen die folgenden Systemkonten auf dem Microsoft Exchange-Server vorhanden sein:

Das Installationskonto

Verwenden Sie das Installationskonto, um sich bei dem Computer anzumelden, auf dem Sie GroupShield für Exchange installieren möchten. Das Konto muß über folgendes verfügen:

- Die Rolle des Dienstkontos „Admin“ für Microsoft Exchange auf Organisation-, Standort- und Konfigurationsebene.
- Domänenadministrator-Rechte für den Windows NT-Server, auf dem Microsoft Exchange ausgeführt wird.

Das Dienstkonto

GroupShield für Exchange verwendet zur Durchführung seiner Virenerkennungsaktivitäten ein Dienstkonto. Das Konto muß über folgendes verfügen:

- Die Rolle des Dienstkontos „Admin“ für Microsoft Exchange.
- Microsoft Windows NT Server-Rechte zur Anmeldung als Dienst, zur Einbindung als Teil des Betriebssystems und zum Anlegen von Sicherheitskopien für Dateien und Verzeichnisse.

Serveranforderungen

Die folgenden Anforderungen basieren auf der Annahme, daß Microsoft Exchange-Server v5.5 und Service Pack 3 auf Ihrem System installiert sind und korrekt funktionieren, bevor Sie GroupShield für Exchange installieren.

Standardserver

	Server auf Intel-Basis
Prozessor	200 MHz Pentium
Arbeitsspeicher	mindestens 64MB
Freier Speicherplatz auf der Festplatte	mindestens 250MB
Betriebssystem	Microsoft Windows NT Server 4.0, Service Pack 4 oder höher, Microsoft Windows 2000 Server
Andere Software	Microsoft Exchange 5.5, Service Pack 3 oder höher.

Unternehmensserver

	Server auf Intel-Basis
Prozessor	200 MHz Pentium
Arbeitsspeicher	mindestens 128MB
Freier Speicherplatz auf der Festplatte	mindestens 250MB
Betriebssystem	Microsoft Windows NT Server 4.0 Enterprise Edition, Service Pack 4 oder höher, Microsoft Windows 2000 Advanced Server
Andere Software	Microsoft Exchange 5.5, Service Pack 3 oder höher.

Sonstige Voraussetzungen

Auf dem Microsoft Exchange-Server müssen außerdem diese Elemente vorhanden sein:

- Der private Informationsspeicher (PRIV.EDB)
- Der folgende Hotfix, um zu verhindern, daß die Microsoft Virus Scan-API einen Scanvorgang bei Zugriff vorzeitig abbricht:

  http://www.microsoft.com/downloads/release.asp?releaseID=20910

- Informationen über die von diesem Hotfix gelösten Probleme finden Sie auf der folgenden Microsoft-Website:

  http://support.microsoft.com/support/kb/articles/Q248/8/38.asp

Installationscheckliste

Bevor Sie GroupShield für Exchange installieren, sollten Sie die folgende Checkliste durchgehen, um sicherzustellen, daß Ihr System für die Ausführung des Setup-Programms von GroupShield für Exchange hinreichend konfiguriert ist und daß Sie über alle zur Installation des Programms erforderlichen Informationen verfügen.

Stellen Sie sicher, daß Ihr System den folgenden Anforderungen entspricht:

- Sie besitzen administrative Rechte sowohl unter Microsoft Windows NT als auch für den Microsoft Exchange-Server.
- Der Installationscomputer verfügt über ein CD-ROM-Laufwerk – für den Fall, daß Sie vorhaben, GroupShield für Exchange unter Verwendung einer McAfee-CD-ROM zu installieren.
- Der Installationscomputer hat Zugang zur Network Associates-Website, http://www.nai.com - falls Sie planen, GroupShield für Exchange über das Internet herunterzuladen.
- Der Installationscomputer hat mindestens 100**MB** freien Speicherplatz auf der Festplatte für die Installation der Software zur Verfügung.
- Sie kennen den Namen des Microsoft Exchange-Servers, der als Installationsziel dient.
- Sie haben Kennwörter und Zugang zu den Administratorkonten, die Sie bei der Installation verwenden.
- Die Installations- und Dienstkonten, die Sie zur Installation von GroupShield für Exchange verwenden, verfügen über die erforderlichen "Rechte and Berechtigungen" für Ihre Organisation, den Standort, an dem Sie die Software installieren, und für deren Konfiguration.

❑ **ANMERKUNG:** Sie können das Installationskonto als Dienstkonto verwenden.

- Sie kennen die Kontennamen anderer Administratoren in Ihrer Organisation, die Zugang zum Quarantäneort haben, an dem GroupShield für Exchange nach Ihren Vorgaben infizierte E-Mail-Nachrichten und -Anlagen speichert.

- Sie kennen den Namen des Postfachs oder die Namen der Postfächer, welche(s) eine Benachrichtigung erhalten, wenn GroupShield für Exchange ein Virus aufspürt.
- Wenn Sie vorhaben, nach Installation von GroupShield für Exchange einen geplanten Scanvorgang auf Anforderung durchzuführen, sollten Sie hierfür eine geeignete Zeit ermittelt haben.

  Führen Sie nach der Installation von GroupShield möglichst bald einen Scanvorgang auf Anforderung aus, um sicherzustellen, daß der Microsoft Exchange-Informationsspeicher virenfrei ist. Planen Sie die Ausführung des Scanvorgangs für einen Zeitraum, in dem die Serveraktivität gering ist.

Installieren von GroupShield für Exchange

Die Installationsschritte in diesem Abschnitt beschreiben, wie Sie GroupShield für Exchange auf einem einzelnen Microsoft Exchange-Server installieren, auf dem GroupShield für Exchange 4.0.4 noch nicht installiert ist. In diesem Fall *muß* Microsoft Exchange auf dem Installationsserver ausgeführt werden, während Sie GroupShield für Exchange installieren.

Informationen über andere GroupShield für Exchange-Installationsszenarien finden Sie hier:

- “McAfee-Supportdienste“ auf Seite 273 Hier erfahren Sie, wie Sie GroupShield für Exchange in einer Microsoft Cluster Server-Konfiguration unter Windows NT Server 4.0 installieren können.
- Weitere Informationen über die Installation der Version 4.5 von GroupShield für Exchange auf einem Computer, auf dem bereits die Version 4.0.4 installiert ist, finden Sie unter “Aktualisieren von GroupShield für Exchange“ auf Seite 51.

WICHTIG: McAfee empfiehlt, daß Sie nicht versuchen, von einer GroupShield für Exchange v4.5 Beta- oder Release Candidate-Version auf die GroupShield für Exchange v4.5-Software zu aktualisieren.

- Technische Dokumente, die beschreiben, wie GroupShield für Exchange auf mehreren Servern oder im Hintergrund installiert wird, finden Sie auf der Network Associates-Website. Oder wenden Sie sich an Ihren McAfee “Technischer Support”-Händler.

Um GroupShield für Exchange von Ihrem gewählten Installationsmedium auf den Computer zu überspielen und zu installieren, führen Sie die folgenden Schritte aus:

1. Starten Sie den Computer, und wählen Sie eine der folgenden Optionen, um die Installationsdatei SETUP.EXE zu finden:

- Legen Sie die McAfee-Installations-CD in das CD-ROM-Laufwerk ein, und führen Sie die folgenden Teilschritte aus:

    a. Klicken Sie in der Windows NT-Task-Leiste auf **Start**, und wählen Sie dann **Ausführen**.

    b. Klicken Sie auf **Durchsuchen**, und suchen Sie dann im Verzeichnis von GroupShield für Exchange nach der Datei SETUP.EXE.

- Legen Sie ein temporäres Verzeichnis auf Ihrer Festplatte an, und führen Sie die folgenden Teilschritte aus:

    a. Stellen Sie eine Verbindung mit der Network Associates-Website her, und laden Sie die Archivdateien von GroupShield für Exchange in dieses Verzeichnis herunter.

    b. Extrahieren Sie die archivierten Ordner in das temporäre Verzeichnis. Die zur Extrahierung von .ZIP-Dateien benötigten Dienstprogramme können Sie über die meisten Onlinedienste erhalten.

> **WICHTIG:** Bei der Installation werden Sie möglicherweise an zwei Stellen gebeten, den Server neu zu starten: einmal zur Installation des Microsoft Windows Installers, wenn dieser auf dem Installationsserver noch nicht on lässt, und einmal um sicherzustellen, daß der Scanner auf Anforderung korrekt funktioniert. Weitere Informationen über die Notwendigkeit dieser Neustarts finden Sie auf der Network Associates-Website. Oder wenden Sie sich an Ihren McAfee "Technischer Support"-Händler.

2. Doppelklicken Sie auf **SETUP.EXE**, um die Installation von GroupShield für Exchange zu starten.

   Um die Datei SETUP.EXE zu finden, durchsuchen Sie entweder das von Ihnen angelegte temporäre Verzeichnis oder das Verzeichnis von GroupShield für Exchange auf der McAfee Installations-CD.

   Nach Abschluß der Initialisierung von Windows Installer klicken Sie innerhalb des Begrüßungsbildschirms (Abbildung 2-1) auf **Weiter>,** um mit der Installation zu beginnen.

McAfee(r) GroupShield(r) für Exchange Setup
MCAFEE
GroupShield
Exchange
Willkommen beim McAfee GroupShield für Exchange Installation Wi...
Beenden Sie zunächst alle Windows-Programme, bevor Sie dieses Installationsprogramm ausführen.
Klicken Sie auf 'Abbrechen', um die Installation zu beenden, und schließen Sie alle geöffneten Programme. Um mit der Installation fortzufahren, klicken Sie auf 'Weiter'.
WARNUNG: Diese Anwendung ist durch Urheberrecht und internationale Vereinbarungen geschützt.
Unberechtigte Reproduktion oder nicht autorisierter Vertrieb dieser Anwendung wird gerichtlich verfolgt und kann zu erheblichen Strafen führen und Schadenersatzforderungen zur Folge haben.
< Zurück
Weiter >
Abbrechen

Abbildung 2-1. GroupShield für Exchange - Begrüßungsbildschirm

3. Lesen Sie den McAfee-Softwarelizenzvertrag. Akzeptieren Sie die Lizenzbedingungen, und klicken Sie auf **Weiter>**, um fortzufahren.

   Wenn Sie mit den Lizenzbestimmungen nicht einverstanden sind, kann die Installation nicht fortgesetzt werden.

4. Lesen Sie den Text im README-Informationsfenster. McAfee empfiehlt Ihnen, die gesamte Datei sorgfältig durchzulesen. Sie enthält wichtige „Last-Minute“-Informationen.

   Klicken Sie auf **Weiter>**, um fortzufahren.

5. Geben Sie im Bildschirm Benutzerinformationen (Abbildung 2-2) Ihren eigenen Namen und den Firmennamen in die dafür vorgesehenen Textfelder ein, und klicken Sie auf **Weiter>**, um fortzufahren.

Abbildung 2-2. GroupShield für Exchange - Installationsbildschirm „Benutzerinformationen“

6. Geben Sie auf dem Bildschirm Server-Setup (Abbildung 2-3 auf Seite 37) den Server und das Verzeichnis an, in dem Sie GroupShield für Exchange installieren möchten.

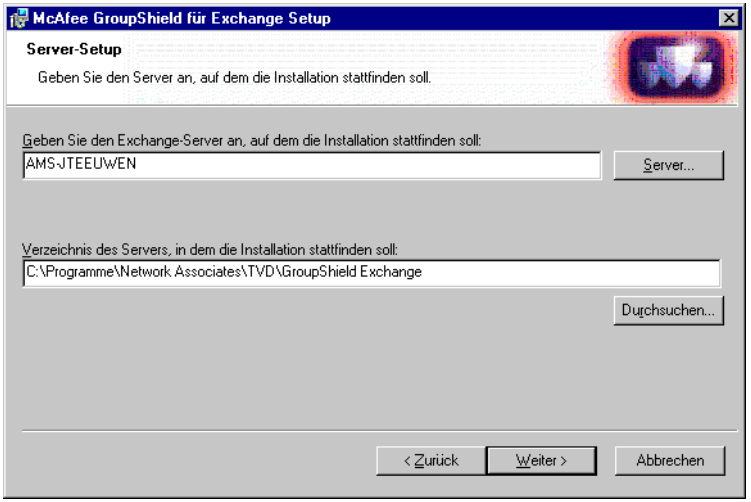

McAfee GroupShield für Exchange Setup
Server-Setup
Geben Sie den Server an, auf dem die Installation stattfinden soll.
Geben Sie den Exchange-Server an, auf dem die Installation stattfinden soll:
AMS-JTEEUWEN
Server...
Verzeichnis des Servers, in dem die Installation stattfinden soll:
C:\Programme\Network Associates\TVD\GroupShield Exchange
Durchsuchen...
< Zurück
Weiter >
Abbrechen

Abbildung 2-3. GroupShield für Exchange - Installationsbildschirm „Server-Setup“

7. Um einen anderen als den auf dem Bildschirm aufgelisteten Microsoft Exchange-Server zu wählen, klicken Sie auf **Server** und wählen unter Verwendung des Dialogfelds Computer auswählen (Abbildung 2-4) den Zielserver aus. Klicken Sie auf **OK**, um zum Bildschirm Server-Setup zurückzukehren.

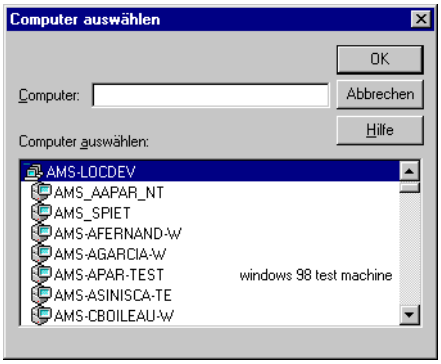


Abbildung 2-4. Installationsbildschirm „Server-Setup“ - Dialogfeld „Computer auswählen“

Wenn Sie GroupShield für Exchange in einem anderen Verzeichnis installieren möchten, klicken Sie auf **Durchsuchen** und verwenden das Dialogfeld Nach Ordner suchen (Abbildung 2-5 auf Seite 38), um das gewünschte Verzeichnis auszuwählen. Klicken Sie auf **OK**, um zum Bildschirm Server-Setup zurückzukehren.

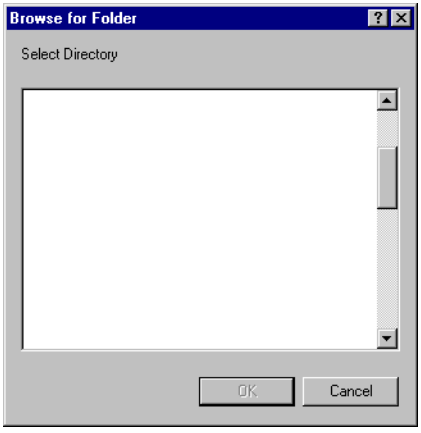


Abbildung 2-5. Fenster „Server-Setup“ - Dialogfeld „Nach Ordner suchen“

8. Klicken Sie auf **Weiter>**, um fortzufahren. Das Setup von GroupShield für Exchange fragt den Server nach vorhandenen Konfigurationsinformationen ab und gibt eine Meldung aus, wenn es eine frühere Version von GroupShield für Exchange auf dem Computer findet.

   Wenn es die vorgefundene Version nicht upgraden kann, haben Sie die Möglichkeit, ihre Konfigurationseinstellungen beizubehalten. Wählen Sie aus, ob Sie die Einstellungen beibehalten wollen, und klicken Sie auf **OK**, um fortzufahren. Die vorhandene Version wird im späteren Verlauf der Installation vom System entfernt.

   ANMERKUNG: Unter "Aktualisieren von GroupShield für Exchange" auf Seite 51 finden Sie Informationen über die Auswirkungen, die die Aktualisierung von einer Version von GroupShield für Exchange auf eine andere auf Ihr System haben kann.

   ---

9. Wählen Sie auf dem Bildschirm Administratorsetup (Abbildung 2-6 auf Seite 39) das Administratorkonto aus, das Sie zur Verwaltung von GroupShield für Exchange und der Ausführung der Dienste von GroupShield für Exchange verwenden möchten.

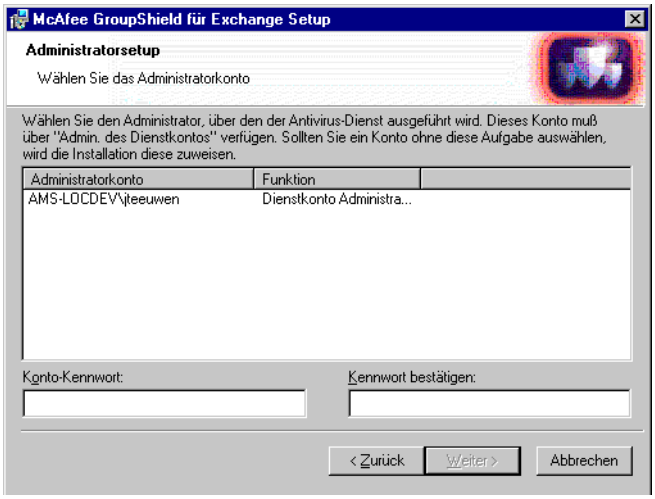

McAfee GroupShield für Exchange Setup
Administratorsetup
Wählen Sie das Administratorkonto
Wählen Sie den Administrator, über den der Antivirus-Dienst ausgeführt wird. Dieses Konto muß über "Admin. des Dienstkontos" verfügen. Sollten Sie ein Konto ohne diese Aufgabe auswählen, wird die Installation diese zuweisen.
Administratorkonto
Funktion
AMS-LOCDEV\jteeuwen
Dienstkonto Administra...
Konto-Kennwort:
Kennwort bestätigen:
< Zurück
Weiter >
Abbrechen

Abbildung 2-6. GroupShield für Exchange - Installationsbildschirm „Administratorsetup"

10. Geben Sie das Kennwort des Kontos ein. Geben Sie es dann ein zweites Mal ein, um es zu bestätigen.

Der Windows Installer fragt von der Netzwerkdomäne eine Liste der Administratoren mit Dienstkonto-Administratorrechten für GroupShield für Exchange ab. Klicken Sie auf **Weiter>**, um fortzufahren.

11. Geben Sie auf dem Bildschirm Quarantäne-Setup (Abbildung 2-7) das Medium an, das GroupShield für Exchange zur Isolierung blockierter oder infizierter E-Mail-Nachrichten und -Anlagen verwenden soll.

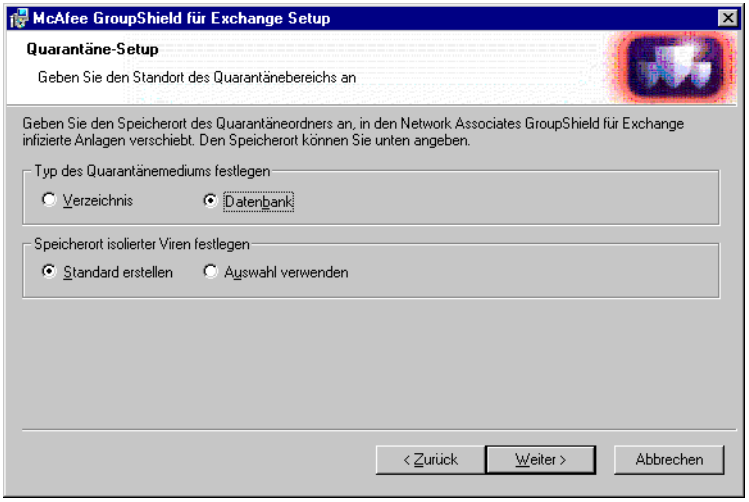

McAfee GroupShield für Exchange Setup
Quarantäne-Setup
Geben Sie den Standort des Quarantänebereichs an
Geben Sie den Speicherort des Quarantäneordners an, in den Network Associates GroupShield für Exchange infizierte Anlagen verschiebt. Den Speicherort können Sie unten angeben.
Typ des Quarantänemediums festlegen
Verzeichnis
Datenbank
Speicherort isolierter Viren festlegen
Standard erstellen
Auswahl verwenden
< Zurück
Weiter >
Abbrechen

Abbildung 2-7. GroupShield für Exchange - Installationsbildschirm „Quarantäne-Setup“

Sie haben die Wahl zwischen:

- **Verzeichnis**

  Diese Option bewirkt lediglich die Auflistung der isolierten Dateien in einem Unterverzeichnis des Programmverzeichnisses von GroupShield für Exchange. Der Verzeichnispfad kann zu einem späteren Zeitpunkt auf der Registerkarte Administration geändert werden.

- **Datenbank**

  Diese Option ermöglicht es Ihnen, isolierte Objekte durch McAfee Quarantine Manager zu inspizieren. Sie können die Datei unter Verwendung der Option **Auswahl verwenden** umbenennen.

12. Klicken Sie auf **Weiter>**, um den Standardort für das gewählte Quarantänemedium zu akzeptieren, oder klicken Sie auf **Ausgewählten verwenden**, um im Dialogfeld Nach Ordner suchen zu einem Ort Ihrer Wahl zu navigieren und ihn als Quarantäneverzeichnis anzugeben. Oder geben Sie im Dialogfeld Datenbank auswählen den Ort des McAfee Quarantine Managers an.

13. Geben Sie auf dem Bildschirm Benutzerbenachrichtigungs-Setup (Abbildung 2-8) an, über welche Postfächer Sie Benachrichtigungen von gefundenen Viren empfangen möchten.

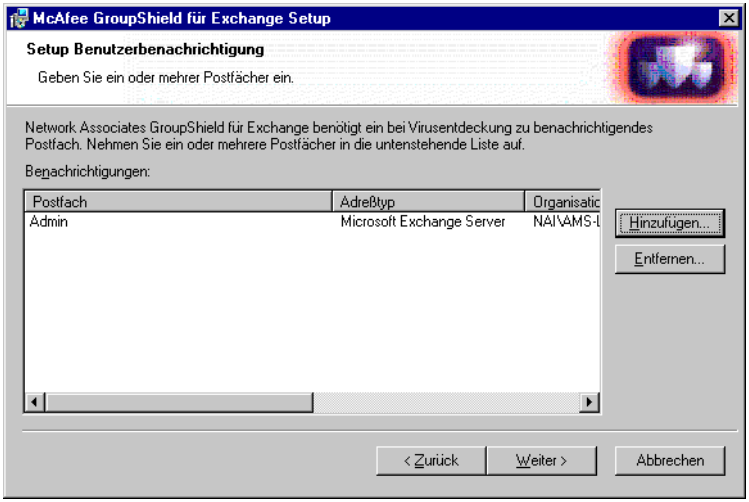


Abbildung 2-8. GroupShield für Exchange - Installationsbildschirm „Benutzerbenachrichtigungs-Setup“

Um ein Postfach zur Liste der Benachrichtigungen hinzuzufügen, führen Sie die folgenden Teilschritte aus:

a. Klicken Sie auf **Hinzufügen...**, und wählen Sie im Dialogfeld Benachrichtigungen auswählen (Abbildung 2-9) die Empfänger aus, die Sie benachrichtigen möchten.

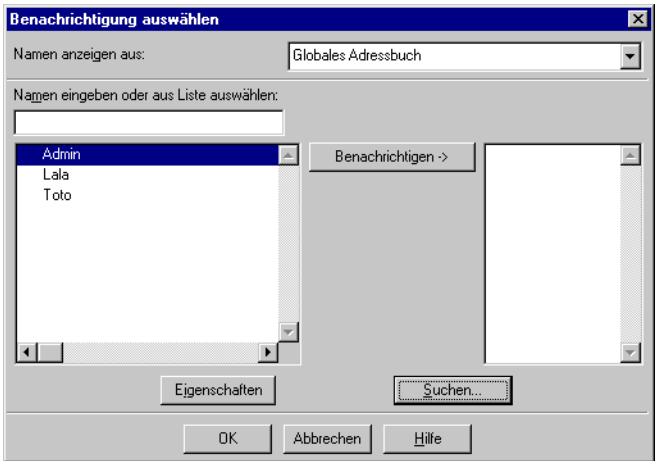


Abbildung 2-9 Installationsbildschirm „Benutzerbenachrichtigungs-Setup“ - Dialogfeld „Benachrichtigung auswählen“

b. Klicken Sie auf **Benachrichtigen>**, um sie zur Liste der Benachrichtigungen hinzuzufügen.

c. Klicken Sie auf **OK**, um zum Bildschirm Benutzerbenachrichtigungs-Setup zurückzukehren.

Klicken Sie auf **Weiter>**, um fortzufahren.

14. Wählen Sie auf dem Bildschirm Zeitplan-Setup (Abbildung 2-10 auf Seite 43) eine der folgenden Optionen zur Zeitplanung eines Scanvorgangs auf Anforderung aus.

- Verwenden Sie die Pfeilsymbole, um Datum und Zeit auszuwählen und damit festzulegen, wann GroupShield für Exchange den Microsoft Exchange-Server scannen soll.
- Wählen Sie die Option **Nach Abschluß der Installation**, um den Scanvorgang unmittelbar im Anschluß an die Installation der Software durchzuführen.

ANMERKUNG: Führen Sie nach der Installation von GroupShield für Exchange möglichst bald einen Scanvorgang auf Anforderung aus, um sicherzustellen, daß der Microsoft Exchange-Informationsspeicher virenfrei ist. McAfee empfiehlt, daß Sie den Scanvorgang so planen, daß er bei niedrigem Serveraufkommen ausgeführt wird.

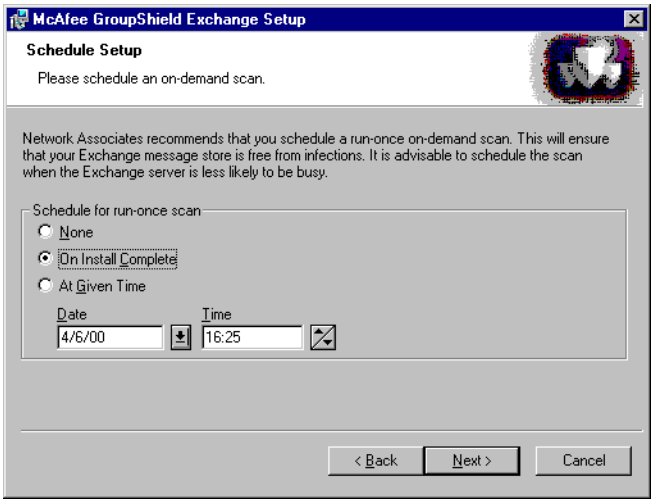

McAfee GroupShield Exchange Setup
Schedule Setup
Please schedule an on-demand scan.
Network Associates recommends that you schedule a run-once on-demand scan. This will ensure that your Exchange message store is free from infections. It is advisable to schedule the scan when the Exchange server is less likely to be busy.
Schedule for run-once scan
None
On Install Complete
At Given Time
Date
4/6/00
Time
16:25
< Back
Next >
Cancel

Abbildung 2-10. GroupShield für Exchange - Installationsbildschirm „Zeitplan-Setup“

15. Klicken Sie auf **Weiter>**, um fortzufahren.
16. Überprüfen Sie die Details der Installation von GroupShield für Exchange auf der Bildschirmseite Zusammenfassung (Abbildung 2-11).

    Wenn die gezeigten Information korrekt sind, klicken Sie auf **Weiter>**, um fortzufahren.

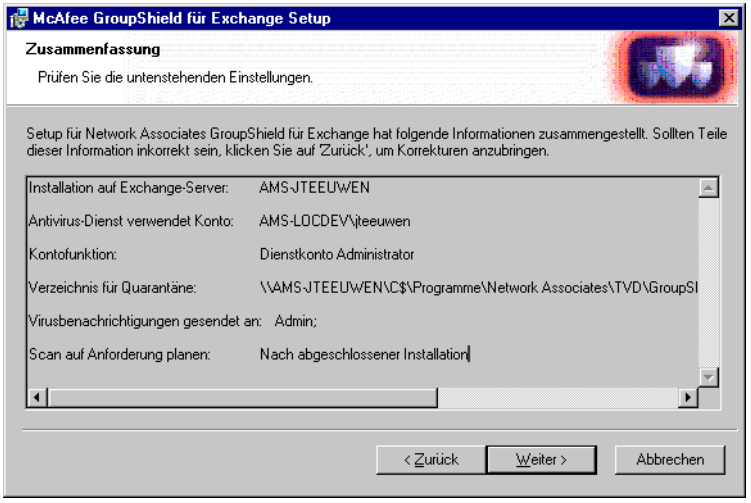

McAfee GroupShield für Exchange Setup
Zusammenfassung
Prüfen Sie die untenstehenden Einstellungen.
Setup für Network Associates GroupShield für Exchange hat folgende Informationen zusammengestellt. Sollten Teile dieser Information inkorrekt sein, klicken Sie auf 'Zurück', um Korrekturen anzubringen.
Installation auf Exchange-Server: AMS-JTEEUWEN
Antivirus-Dienst verwendet Konto: AMS-LOCDEV\jteeuwen
Kontofunktion: Dienstkonto Administrator
Verzeichnis für Quarantäne: \\AMS-JTEEUWEN\C$\Programme\Network Associates\TVD\GroupSI
Virusbenachrichtigungen gesendet an: Admin;
Scan auf Anforderung planen: Nach abgeschlossener Installation
< Zurück
Weiter >
Abbrechen

Abbildung 2-11. GroupShield für Exchange - Installationsbildschirm „Zusammenfassung“

17.). Klicken Sie erneut auf **Weiter>**.

18. Klicken Sie im nächsten Bildschirm auf **Installieren**, um zu bestätigen, daß Sie nun zur Installation von GroupShield für Exchange bereit sind.

19. Wenn alle Dateien kopiert wurden, klicken Sie auf **Fertig stellen**. Sie müssen den Computer neu starten, wenn Sie dazu aufgefordert werden.

    Auf Seite 50 können Sie erfahren, wie Sie die Serververwaltungskonsole GroupShield-Eigenschaften öffnen.

Informationen über die Installation der Version v4.5 von GroupShield für Exchange auf einem Computer, auf dem bereits die Version v4.0.4 installiert ist, finden Sie unter “Aktualisieren von GroupShield für Exchange“ auf Seite 51.

Testen einer Installation

Nach der Installation ist GroupShield für Exchange bereit, Ihr System nach infizierten Dateien zu durchsuchen. Sie können testen, ob das Programm richtig installiert wurde und ordnungsgemäß nach Viren suchen kann, indem Sie einen Test durchführen, der von EICAR (European Institute of Computer Anti-virus Research), einem Zusammenschluß von Virenschutzanbietern mit Hauptsitz in Europa, als Methode für ihre Kunden zum Testen einer beliebigen Virenschutzsoftware-Installation entwickelt wurde.

Sie sollten die EICAR-Testdatei verwenden, um sowohl den GroupShield für Exchange-Scanner bei Zugriff als auch den GroupShield für Exchange-Scanner auf Anforderung zu testen.

Führen Sie folgende Schritte aus, um eine Installation zu testen:

1. Öffnen Sie einen normalen Texteditor, und geben Sie folgende Zeile ein:

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS
   -TEST-FILE!$H+H*
   ```

   ❑ **ANMERKUNG:** Die oben gezeigte Zeile muß im Fenster Ihres Texteditors als **eine Zeile** erscheinen. Wenn Sie dieses Handbuch auf Ihrem Computer lesen, können Sie die Zeile direkt aus der Adobe Acrobat-Datei (.PDF-Datei) in Ihren Texteditor kopieren.

2. Speichern Sie die Datei unter dem Namen EICAR.COM. Die Datei wird 68 oder 70 Bytes groß sein.

3. Starten Sie Ihre E-Mail-Clientsoftware. Legen Sie eine neue E-Mail-Nachricht an, und fügen Sie die Datei EICAR.COM ein. Wählen Sie dann eine der folgenden Optionen und führen Sie die jeweils zugehörigen Teilschritte aus:

- So testen Sie den Scanner bei Zugriff von GroupShield für Exchange:

  a. Senden Sie die Nachricht, welche die Datei EICAR.COM enthält, an ein Postfach auf dem Server mit GroupShield für Exchange.

     Der Scanner bei Zugriff teilt mit, daß er die EICAR.COM-Testdatei gefunden hat.

- So testen Sie den Scanner auf Anforderung von GroupShield für Exchange:

  a. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Bei Zugriff.

  b. Wählen Sie im Feld **Bei Viruserkennung zu ergreifende Maßnahme** die Option **Infektion protokollieren und weiter ohne Säuberung**.

  c. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

  d. Als nächstes senden Sie die Nachricht, die die Datei EICAR.COM enthält, an ein Postfach auf dem Server mit GroupShield für Exchange.

  e. Kehren Sie zur Serververwaltungskonsole GroupShield-Eigenschaften zurück, und klicken Sie auf die Registerkarte Auf Anforderung.

  f. Konfigurieren Sie einen Scanvorgang auf Anforderung für das Postfach, das die Nachricht mit der Datei EICAR.COM enthält.

     Das Verfahren zur Konfigurierung eines Scanvorgangs auf Anforderung ist im Abschnitt Kapitel 4, „Scanvorgänge auf Anforderung“ beschrieben.

     GroupShield für Exchange meldet, daß die Testdatei EICAR.COM im McAfee Log Manager entdeckt wurde.

     Anleitungen zum Öffnen und Konfigurieren des Dienstprogramms Log Manager finden Sie unter Kapitel 6, „Serveradministration und Protokollierung“.

WICHTIG: Die EICAR-Testdatei **enthält kein Virus**, sie ist also nicht in der Lage, sich auf andere Dateien auszubreiten oder sie zu infizieren oder auf andere Weise Ihr System negativ zu beeinträchtigen. Löschen Sie die Datei, nachdem Sie Ihre Installation getestet haben, um zu vermeiden, daß andere Benutzer alarmiert werden. Aktivieren Sie eine andere Option für die Aktion, die GroupShield für Exchange unternehmen soll, wenn bei einem Scanvorgang bei Zugriff ein Virus entdeckt wird.

Änderungen am System nach Abschluß der Installation

Wenn GroupShield für Exchange zum ersten Mal auf Ihrem System installiert wurde, können Sie feststellen, daß in Ihrem System die folgenden Änderungen vorgenommen wurden:

- Ein verborgener Empfänger namens **GroupShield für Exchange (Servername)** wurde in den Empfängercontainer eingefügt. Ihrer Microsoft Exchange-Dokumentation können Sie entnehmen, wie Sie einen verborgenen Empfänger anzeigen.
- Die McAfee Quarantine Manager-Datenbank bzw. das Quarantäneverzeichnis werden auf Ihrem Microsoft Exchange-Server erstellt – je nachdem, für welche Option Sie sich entschieden haben.
- Gegebenfalls wird ein neuer Ordner des Typs **Organisation(<Sprachkennung>)** auf dem Microsoft Exchange-Server angelegt.

  Zwei Globale Formulare werden in dem Formularordner des Programmverzeichnisses von GroupShield für Exchange abgelegt. Sie dienen zur Anzeige der Virenschutzberichte von GroupShield für Exchange. Eine Beschreibung der Formulare und ihrer Aktionen finden Sie unter “Globale Formulare von GroupShield für Exchange“ auf Seite 47.
- Das folgende Add-In wird zum Microsoft Exchange Administrator-Verzeichnis Add-ins hinzugefügt: \Network Associates GroupShield Exchange Server Administration for i386.

  Dieses Add-In ermöglicht es Ihnen, GroupShield für Exchange mit dem Microsoft Exchange-Administratorprogramm zu verwalten.
- Zum Verzeichnis \Exchsrvr\Add-ins wird das folgende Unterverzeichnis hinzugefügt: NAISAdm.
- Die Dienste von GroupShield für Exchange werden zum Dienstefenster der Systemsteuerung hinzugefügt. Die folgenden Dienste werden bei Installation von GroupShield für Exchange automatisch gestartet:
  - Network Associates GroupShield für Exchange

    Der Dienst GroupShield für Exchange ist vom Microsoft-Informationsspeicher abhängig.
  - Network Associates GroupShield-Online-Aktualisierung

    Der GroupShield Onlineaktualisierungs-Dienst ist vom Microsoft-Informationsspeicher und dem Dienst GroupShield für Exchange abhängig.

– Network Associates Log Service (Protokollierdienst)

– Network Associates Warnungs-Manager

  Der Warnungs-Manager-Dienst existiert möglicherweise bereits auf Ihrem System, wenn Sie ein anderes McAfee-Virenschutzprogramm verwenden.

– Network Associates Outbreak Manager

  Der Network Associates Outbreak Manager-Dienst ist abhängig vom Network Associates-Protokollierdienst. Der Outbreak Manager-Dienst wird bei der Installation von GroupShield für Exchange automatisch mitinstalliert. Er fungiert als Microsoft Windows-Dienst und erlaubt Ihnen auf diese Weise eine kontinuierliche Überwachung Ihres Computers. Der Outbreak Manager-Dienst existiert möglicherweise bereits auf Ihrem System, wenn Sie ein anderes McAfee-Virenschutzprogramm verwenden.

ANMERKUNG: Gelegentlich kann es erforderlich sein, einen der Dienste von GroupShield für Exchange zu beenden und neu zu starten, damit die Wirkungen einer bestimmten Aktion in Kraft treten können. Wie Sie dabei vorgehen, erfahren Sie im Abschnitt “Beenden und Neustart der Dienste“ auf Seite 48.

Ergänzende Informationen

Globale Formulare von GroupShield für Exchange

Globale Formulare sind ausführbare Dateien, die Sie in Microsoft Exchange zur Anzeige benutzerdefinierter Nachrichten oder auch zur Ausführung benutzerdefinierter Funktion verwenden können. GroupShield für Exchange speichert zwei solcher Formulare im Stammverzeichnis des Programmordners von GroupShield für Exchange. Die neuen Geschäftsbereiche lauten:

- Das Formular für den Virenschutzbericht namens **AVform**. Je nach Konfiguration der Benachrichtigungen verwendet GroupShield für Exchange das Formular AVform, um optional Administratoren, vorgesehene Empfänger und den Nachrichtenabsender zu warnen, wenn während eines Scanvorgangs auf Anforderung eine infizierte Datei oder Anlage entdeckt wird. Das Formular wird auch bei einem Scanvorgang bei Zugriff verwendet, um einen Administrator über eine Infektion zu informieren.

- Das Formular für einen zusammenfassenden Bericht mit der Bezeichnung **Sumform**. GroupShield für Exchange sendet das Formular mit der Zusammenfassung an Administratoren, um ihnen die Ergebnisse eines geplanten Scanvorgangs auf Anforderung mitzuteilen.

Die Quarantäneorte

GroupShield für Exchange bietet zwei Methoden zur Isolierung infizierter oder blockierter Nachrichten oder Anlagen, für die weitere Aktionen vorgesehen sind:

- Die **McAfee Quarantine Manager**-Datenbank. Sie wird standardmäßig unter dem folgenden Pfad abgelegt:

  ```
  C:\Programme\Network Associates\Tvd\GroupShield Exchange
  \i386\Quarantine\QTINE.MDB
  ```

- Das Quarantäneverzeichnis. Ist standardmäßig der folgende Pfad:

  ```
  C:\Programme\Network Associates\Tvd\GroupShield Exchange
  \1386\Quarantine\<Standort>#<Server>
  ```

Das Quarantäneverzeichnis enthält die Details zu jedem isolierten Element, z. B. den Namen der Datei und den Namen des Virus, in einer Header-Datei. Die Header-Datei enthält auch die isolierte Anlage. McAfee empfiehlt, daß Sie mit allen isolierten Anlagen sehr vorsichtig umgehen und diese nicht an andere Personen weiterleiten, es sei denn, Sie sind sich absolut sicher, daß die jeweilige Anlage nicht infiziert ist.

Wenn Sie die Quarantänefunktion aktivieren möchten, führen Sie eine der Quarantäneaktionen durch, die im Feld Bei Viruserkennung zu ergreifende Maßnahme angezeigt werden. Auf Seite 79 finden Sie Informationen über die Quarantäneaktionen im Rahmen von Scanvorgängen auf Anforderung, und auf Seite 65 können Sie erfahren, welche Quarantäneaktionen während eines Scanvorgangs bei Zugriff möglich sind.

❑ **ANMERKUNG:** Um die Quarantänefunktion zu deaktivieren, aktivieren Sie eine der beiden folgenden Optionen (**Anlage löschen, wenn Säuberung fehlschlug** oder **Anlage ohne Desinfektion löschen**) auf den Registerkarten Bei Zugriff und Auf Anforderung.

Anfordern von Hilfeinformationen über GroupShield für Exchange

Um die Merkmale und Funktionen der Serververwaltungskonsole GroupShield-Eigenschaften und anderer Komponenten von GroupShield für Exchange kennenzulernen, klicken Sie in einer beliebigen Registerkarte auf **Hilfe**.

Beenden und Neustart der Dienste

Gelegentlich kann es erforderlich sein, die Dienste von GroupShield für Exchange zu beenden und neu zu starten, damit die Wirkungen einer bestimmten Aktion oder Änderung in Kraft treten. Ein Beispiel dafür wäre die Festlegung des Zeitlimits für das Scannen, um eine Dienstverweigerung

(denial-of-service) zu vermeiden. In der Regel hilft das Programm mit entsprechenden Hinweisen, falls es erforderlich wird, die Dienste zu beenden.

Auf Seite 46 finden Sie eine Beschreibung der McAfee-Dienste, aus denen sich GroupShield für Exchange zusammensetzt.

Um die Dienste von GroupShield für Exchange zu beenden und neu zu starten, führen Sie die folgenden Schritte aus:

1. Klicken Sie in Windows NT auf **Start**, und zeigen Sie dann auf **Einstellungen**. In Windows 2000 klicken Sie auf **Start**, zeigen Sie auf **Programme**, und wählen Sie die Option **Verwaltungsprogramme**. Klicken Sie dann auf **Dienste**.
2. Klicken Sie auf **Systemsteuerung**, und doppelklicken Sie dann auf das **Dienste**-Symbol.

   Das Dialogfeld Dienste erscheint und zeigt eine Auflistung aller aktuell ausgeführten Dienste an (Abbildung 2-12).

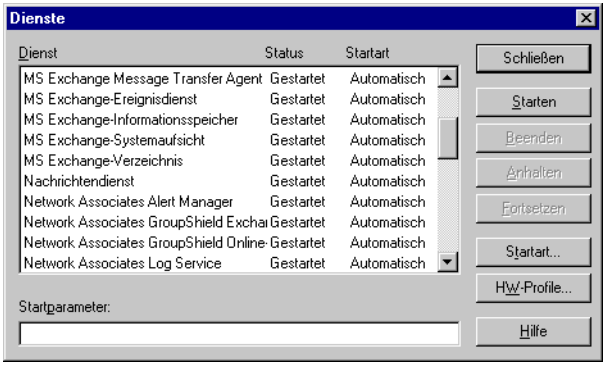


Abbildung 2-12. Systemsteuerung - Option „Dienste“

3. Klicken Sie auf den Dienst, den Sie beenden möchten, und dann auf **Beenden**.
4. Klicken Sie auf **OK**, um zu bestätigen, daß Sie den gewählten Dienst beenden möchten.

   Warten Sie, bis der Dienst beendet ist. Zu diesem Zeitpunkt sollte der Eintrag für den Dienst in der Spalte Status leer sein.
5. Markieren Sie dann den Dienst in der Liste, und klicken Sie auf **Starten**, um den Dienst von neuem zu starten.

   Warten Sie, bis der Dienst startet. Zu diesem Zeitpunkt sollte der Eintrag für den Dienst in der Spalte Status den Wert Gestartet haben.
6. Klicken Sie auf **Schließen**.

Öffnen der Serververwaltungskonsole GroupShield-Eigenschaften

Die Serversoftware von GroupShield für Exchange wird unter Verwendung des Microsoft Exchange Administrator-Dienstprogramms gestartet.

Um das Dienstprogramm zur Serververwaltung für GroupShield für Exchange zu öffnen, führen Sie folgende Schritte aus:

1. Klicken Sie in der Windows NT-Taskleiste auf **Start**, zeigen Sie auf **Programme**, und klicken Sie auf **Microsoft Exchange**. Wählen Sie anschließend **Microsoft Exchange Administrator**.
2. Navigieren Sie im Exchange Administrator zu dem Server, mit dem Sie sich verbinden möchten, und wählen Sie den Namen des Standortes aus, dessen Konfigurationsdetails Sie öffnen möchten. Klicken Sie auf **Konfiguration**.
3. Klicken Sie auf **Server**, und wählen Sie den Server aus, den Sie konfigurieren möchten. Klicken Sie nun auf **Network Associates GroupShield**. Es wird das Fenster GroupShield-Eigenschaften angezeigt, in dem die Registerkarte **Administration** ausgewählt ist (Abbildung 2-13).

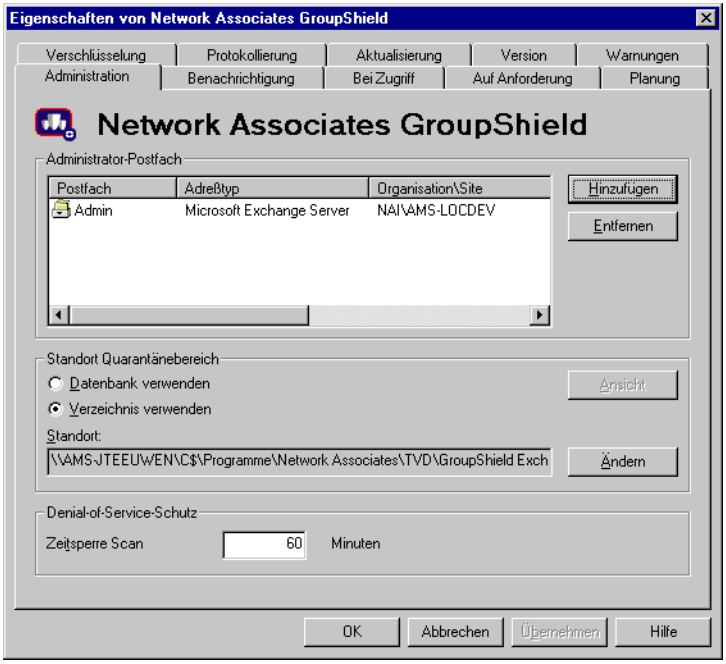


Abbildung 2-13. GroupShield-Eigenschaften - Registerkarte „Administration“

Lesen Sie die folgenden Kapitel dieses Administratorhandbuchs, wenn Sie weitere Einzelheiten über die Verwendung der GroupShield-Eigenschaften erfahren möchten:

- Kapitel 3, „Scanvorgänge „bei Zugriff““ mit Anleitungen zur Konfigurierung von Scanvorgängen „bei Zugriff“.
- Kapitel 4, „Scanvorgänge auf Anforderung“ mit Anleitungen zur Konfigurierung von Scanvorgängen „auf Anforderung“.
- Kapitel 5, „Benachrichtigungen und Alarmmeldungen“ mit Anleitungen zur Konfigurierung der Benachrichtigungs- und Alarmierungsverfahren, die GroupShield für Exchange bei Entdeckung eines Virus verwendet.
- Kapitel 6, „Serveradministration und Protokollierung“ mit Anleitungen zur Verwendung der Registerkarten Administration, Verschlüsselung, Dienstprogramme, Version und Protokollierung.
- Kapitel 7, „Automatische Aktualisierung der .DAT-Dateien“ mit Anleitungen zur Aktualisierung der Virusdefinitionsdateien (.DAT-Dateien) von GroupShield für Exchange.

Aktualisieren von GroupShield für Exchange

Sie können Version 4.5 von GroupShield für Exchange problemlos auf einem Microsoft Exchange-Server installieren, auf dem bereits die Version 4.0.4 von GroupShield für Exchange installiert ist. Der Installationsprozeß ähnelt dem, der unter “Installieren von GroupShield für Exchange“ auf Seite 34 beschrieben ist.

❑ **ANMERKUNG:** Versuchen Sie nicht, von einer GroupShield für Exchange v4.5 Betaversion zu aktualisieren. Wenn Sie an einem Standort auf die GroupShield für Exchange v4.5-Software aktualisiert haben, empfiehlt McAfee außerdem, daß Sie nicht versuchen, die GroupShield für Exchange v4.0.4-Software an diesem Standort erneut zu installieren, da die v4.0.4-Installation Links zu den v4.5-Add-In-Erweiterungen entfernt. Stattdessen sollten Sie die v4.5-Software entfernen, bevor Sie sich an die Neuinstallation der v4.0.4-Software machen.

Um GroupShield für Exchange von der Version 4.0.4 auf die Version 4.5 zu aktualisieren, führen Sie die folgenden Schritte aus:

1. Suchen Sie nach der Datei **SETUP.EXE**, wie unter Schritt 1 auf Seite 35 beschreiben, und doppelklicken Sie darauf.
2. Starten Sie den Server neu, wenn Sie dazu aufgefordert werden.

3. Bestätigen Sie, daß Sie die vorhandenen Einstellungen übernehmen möchten, beispielsweise die Administratorpostfächer und die geplanten Scanvorgänge auf Anforderung.

4. Führen Sie die weiteren Installationschritte aus, wie unter “Installieren von GroupShield für Exchange“ auf Seite 34 beschrieben, bis Sie zum Bildschirm Quarantäne-Setup gelangen.

   Sie müssen bei Verwendung von GroupShield für Exchange 4.5 den Quarantäneort festlegen, da ältere Versionen der Software einen einzigen Quarantäneordner zur Speicherung infizierter Anlagen verwendeten.

5. Der Bildschirm Benutzerbenachrichtigungs-Setup zeigt dieselbe Liste der Administratorpostfächer an, die Sie unter GroupShield für Exchange 4.0.4 angegeben haben. Unter Schritt 13 auf Seite 41 können Sie erfahren, wie Sie Postfächer zur Liste hinzufügen oder aus ihr entfernen.

6. Legen Sie einen Zeitpunkt für den Scanvorgang auf Anforderung fest, der im Anschluß an die Installation erfolgen soll. Benutzen Sie dazu entweder die Pfeilsymbole, oder wählen Sie die Option **Nach Abschluß der Installation**.

   ❑ **ANMERKUNG:** Führen Sie nach der Installation von GroupShield für Exchange möglichst bald einen Scanvorgang auf Anforderung aus, um sicherzustellen, daß der Microsoft Exchange-Informationsspeicher virenfrei ist. McAfee empfiehlt, daß Sie den Scanvorgang so planen, daß er bei niedrigem Serveraufkommen ausgeführt wird.

   ---

7. Überprüfen Sie die Einzelheiten der Konfiguration auf der Bildschirmseite Zusammenfassung, und klicken Sie dann auf **Weiter>**.

8. Nachdem das System aktualisiert worden ist, klicken Sie auf **Ja**, um zu bestätigen, daß Sie die Virenschutzkomponenten aus Ihrem System entfernen möchten. Klicken Sie dann auf **OK**, um die neuen Programmdateien von GroupShield für Exchange zu installieren.

Nachdem die Upgrade-Dateien vollständig installiert sind, werden Sie feststellen, daß die folgenden GroupShield für Exchange v4.0.4-Komponenten auf Ihrem System bleiben. Dies geschieht, da einige Teile von GroupShield für Exchange v4.5 auf Standortebene installiert werden und andere Server möglicherweise weiterhin GroupShield für Exchange v4.04 verwenden:

WICHTIG: McAfee empfiehlt, daß Sie auch bei einem Upgrade auf GroupShield für Exchange v4.5 keinerlei Komponenten der Version v4.0.4 aus dem Exchange Administrator-Verzeichnis Add-ins entfernen. Die Komponenten sind auf Standortebene installiert. Wenn Sie sie entfernen, tritt beim Verwalten von GroupShield für Exchange v4.0.4-Servern, die an diesem Standort verbleiben, ein Fehler auf.

- Bei Benutzerpostfächern, die bereits unter GroupShield für Exchange v4.0.4 bestanden, wird die Registerkarte Virusschutzeinstellungen für die Benutzerverwaltung beibehalten. Weitere Informationen über die Benutzerverwaltung finden Sie im Benutzerhandbuch von GroupShield für Exchange v4.0.4.
- Die Registerkarte Dienstprogramme bleibt auf der Serververwaltungskonsole GroupShield-Eigenschaften. Weitere Informationen über die Optionen der Registerkarte Dienstprogramme finden Sie im Benutzerhandbuch von GroupShield für Exchange v4.0.4.
- Die Registerkarte Aktualisierung der Serververwaltungskonsole GroupShield-Eigenschaften verfügt nun über die Option Clients aktualisieren. Bei dieser Option werden nur diejenigen Clientcomputer aktualisiert, die bereits unter GroupShield für Exchange v4.0.4 definiert waren.
- Die folgenden von GroupShield für Exchange 4.0.4 verwendeten Komponenten verbleiben im Microsoft Exchange Administrator-Standortverzeichnis Add-ins:
  - Network Associates GroupShield Exchange Server Administration for i386

    ANMERKUNG: Die mit GroupShield für Exchange 4.5 installierte Komponente Server Administration i386 hat denselben Namen wie die mit v4.0.4 installierte Komponente.

  - Network Associates GroupShield Exchange Server Administration for Alpha
  - Network Associates GroupShield Exchange User Administration for i386
  - Network Associates GroupShield Exchange User Administration for Alpha.

    ANMERKUNG: Die Komponente User Administration bleibt nicht erhalten, wenn Sie sie bei der ursprünglichen Installation von GroupShield für Exchange v4.0.4 nicht installiert hatten.

Reparieren der Software

Sie können die neue Microsoft Windows Installer-Technologie verwenden, um Ihre GroupShield für Exchange-Installationsdateien, Registrierungsschlüssel und Verknüpfungen neu zu installieren und zu reparieren, wenn sie ungültig werden. Die Reparatur der Software ist in folgenden Fällen angebracht:

- Eine Datei ist veraltet, fehlt oder ist beschädigt

❑ **ANMERKUNG:** Sie können nur fehlende oder beschädigte Dateien reparieren, die in der Spalte Attribute der Tabelle Datei den Eintrag `msidbFileAttributesChecksum` aufweisen. Sie können jedoch veranlassen, daß die Software alle Dateien unabhängig vom Prüfsummenattribut neu installiert. In der Microsoft Windows Installer-Dokumentation werden die Reparaturoptionen der Installer-Technologie ausführlich beschrieben.

- Ein Registrierungsschlüssel muß neu geschrieben werden
- Verknüpfungen oder Symbole müssen neu installiert oder bearbeitet werden.

Gehen Sie wie folgt vor, um GroupShield für Exchange zu reparieren:

1. Navigieren Sie zum GroupShield für Exchange-Installationsort, und doppelklicken Sie auf das Programm **Setup**.
2. Öffnen Sie den Bildschirm Anwendung hinzufügen / entfernen (Abbildung 2-14), und wählen Sie eine der folgenden Möglichkeiten:

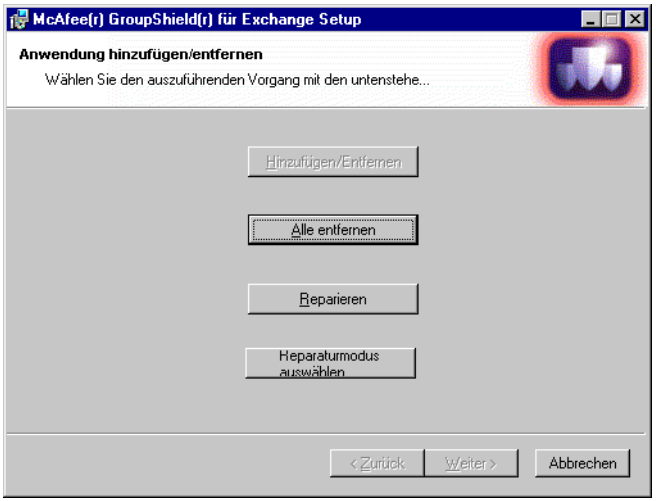


Abbildung 2-14. Windows Installer - Bildschirm „Anwendung hinzufügen/entfernen“

- **Reparieren**, damit der Installer GroupShield für Exchange unter Verwendung der Standardeinstellungen neu installiert.

ACHTUNG: McAfee empfiehlt die Verwendung dieser Option nur, wenn Ihre Kopie von GroupShield für Exchange unwiderruflich zerstört ist. Diese Option ersetzt Ihre GroupShield für Exchange-Konfiguration durch die Einstellungen der ursprünglichen Installation. Notieren Sie alle Einstellungen, die Sie beibehalten möchten, bevor Sie diese Option verwenden, z. B. festgelegte Server, Benachrichtigungseinstellungen, Aktionen, die die Software beim Entdecken eines Virus durchführen soll, und Zeiten geplanter Scanvorgänge.

- **Wählen Sie Reparaturmodus,** um den Bildschirm Setup-Reparaturmodus anzuzeigen.

3. Aktivieren oder deaktivieren Sie Kontrollkästchen, um festzulegen, welche Reparaturoptionen Sie verwenden möchten.

   Standardmäßig repariert GroupShield für Exchange alle Dateien, die als fehlend oder veraltet erkannt werden.

4. Klicken Sie auf **OK**, um zum Bildschirm Anwendung hinzufügen / entfernen zurückzukehren. Klicken Sie dann auf **Reparieren**.

Die Software aktualisiert Ihr System, damit es die reparierten Objekte verwendet.

Entfernen der Software mit dem Windows Installer

Der Microsoft Windows Installer ermöglicht das problemlose Entfernen von GroupShield für Exchange, wobei das Setup-Programm selbst verwendet wird.

ACHTUNG: Nach dem Entfernen von GroupShield für Exchange sind Ihre Benutzer allerdings ohne Schutz gegen Virusangriffe, die von infizierten E-Mail-Nachrichten und -Anlagen weiterverbreitet werden. Entfernen Sie das Programm nur dann, wenn Sie sicher sind, daß Sie schnell ein Upgrade auf eine neue Version durchführen können.

Gehen Sie wie folgt vor, um GroupShield für Exchange mit Hilfe des Windows Installers zu entfernen:

1. Suchen Sie nach der Datei **SETUP.EXE**, die Sie zum Installieren von GroupShield für Exchange verwendet haben, und doppelklicken Sie darauf. Warten Sie dann, bis der Windows Installer die auf Ihrem System installierten GroupShield für Exchange-Komponenten gefunden hat.
2. Klicken Sie im Fenster Anwendung hinzufügen / entfernen (Abbildung 2-14 auf Seite 55) auf die Option **Alles entfernen**.
3. Klicken Sie im Fenster Deinstallation (Abbildung 2-15) von McAfee GroupShield für Exchange auf **Weiter>**, um zu bestätigen, daß Sie GroupShield für Exchange von Ihrem System löschen möchten.

McAfee® GroupShield® Exchange Uninstall
MCAFEE
GroupShield
Exchange
McAfee GroupShield
Exchange Uninstall
This will remove McAfee GroupShield Exchange from your machine. Are you sure you want to continue?
Press the Next button to remove the application.
Press the Cancel button to exit the uninstall process.
< Back
Next >
Cancel

Abbildung 2-15. Windows Installer - Bildschirm „Deinstallation“

4. Warten Sie, während das Programm die Dienste von GroupShield für Exchange beendet, GroupShield für Exchange aus Ihrem System entfernt und anschließend Ihr System aktualisiert, um alle Komponenten von GroupShield für Exchange vollständig zu entfernen.

   Dieser Vorgang kann einige Minuten in Anspruch nehmen.

5. Klicken Sie auf **Beenden**, um den Windows-Installationsassistenten zu beenden.

Manuelles Entfernen der Software

Sie können GroupShield für Exchange aus Ihrem System entfernen, indem Sie alle dazugehörigen Dateien und Komponenten löschen. Allerdings rät McAfee zur Verwendung des Windows Installers, wie im vorhergehenden Abschnitt “Entfernen der Software mit dem Windows Installer” beschrieben.

Um die Serveranwendung GroupShield für Exchange von Ihrem Computer zu entfernen, führen Sie die folgenden Schritte aus:

1. Starten Sie den Exchange-Administrator im Basismodus. Öffnen Sie Sie dazu eine Eingabeaufforderung, und geben Sie folgenden Befehl:

   ```
   <exchsrvr directory>\bin\ADMIN.EXE /R
   ```

   an der Eingabeaufforderung ein. Die eckigen Klammern < > brauchen Sie nicht einzugeben.

2. Nach dem Öffnen des Exchange-Administratorprogramms führen Sie die folgenden Schritte aus:

   a. Legen Sie den Server fest, von dem aus Sie die Anwendung entfernen möchten, und wählen Sie dann Network Associates GroupShield. Als nächstes wählen Sie im Menü **Bearbeiten** den Befehl **Basisobjekt löschen**.

   b. Wechseln Sie in das Verzeichnis Add-ins, und löschen Sie dann das darin installierte Add-In **Network Associates GroupShield Exchange Server Administration for i386**.

   c. Wenn außer den GroupShield für Exchange-Formularen keine benutzerdefinierten Formulare im Organisationsformularordner existieren, wählen Sie im Menü **Extras** den Befehl **Formularadministrator**. Wählen Sie im geöffneten Dialogfeld das Formular **Organisation(<Sprachkennung>)**, und klicken Sie dann auf **Entfernen**.

   ACHTUNG: Sofern im Organisations-Formularordner noch Formulare anderer Hersteller oder benutzerdefinierte Formulare existieren, sollte das Formular **Organisation (<Sprachkennung>)** nicht gelöscht werden.

   d. Wählen Sie in Microsoft Exchange Administrator aus dem Menü **Ansicht** die Option **Verborgene Empfänger**, und markieren Sie den Empfänger **GroupShield für Exchange (Servername)**.

      Ignorieren Sie den Fehler, der besagt, daß die Erweiterung NAI Siteserver nicht geladen werden konnte.

   e. Wählen Sie dann im Menü **Bearbeiten** den Befehl **Löschen**.

3. Klicken Sie in der Windows-Taskleiste auf **Start**, zeigen Sie auf Einstellungen, und wählen Sie dann Systemsteuerung. Suchen Sie nach der Option Dienste und doppelklicken Sie darauf, um das entsprechende Fenster der Systemsteuerung zu öffnen.

4. Beenden Sie die folgenden Dienste von GroupShield für Exchange. Informationen über den Neustart von Diensten finden Sie unter “Beenden und Neustart der Dienste“ auf Seite 48:

- Network Associates GroupShield für Exchange
- Network Associates GroupShield-Online-Aktualisierung
- Network Associates Log Service (Protokollierdienst)
- Network Associates Warnungs-Manager

- Network Associates Outbreak Manager

5. Nach dem Beenden der Dienste schließen Sie das Fenster der Systemsteuerung.

6. Starten Sie den Windows-Registrierungs-Editor. Suchen Sie nach den folgenden Registrierungsschlüsseln, und entfernen Sie sie:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVExch32Service

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVUPDService

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Network Associates-Protokollierdienst

   ANMERKUNG: Entfernen Sie diesen Schlüssel nicht, wenn Sie eine Version des Protokollierdienstes oder Outbreak Manager-Dienstes mit Hilfe eines anderen McAfee-Virenschutzprogramms installiert haben.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Outbreak Manager

   ANMERKUNG: Entfernen Sie diesen Schlüssel nicht, wenn Sie eine Version des Outbreak Manager-Dienstes mit Hilfe eines anderen McAfee-Virenschutzprogramms installiert haben.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AlertManager

   HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\AlertManager

   ANMERKUNG: Entfernen Sie diesen Schlüssel nicht, wenn Sie eine Version des Alert Manager-Dienstes mit Hilfe eines anderen McAfee-Virenschutzprogramms installiert haben.

   HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\Shared Components

   ANMERKUNG: Entfernen Sie diesen Schlüssel nicht, wenn Sie eine der aufgelisteten gemeinsamen Komponenten mit anderen McAfee-Virenschutzprodukten verwenden.

   HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\GroupShield Exchange

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BB1BBB21-6A63-43C1-B9E9-15CC1F39B8CC}

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\AVEXCH32.EXE

7. Entfernen Sie schließlich den folgenden Registrierungsschlüssel, sofern Sie zuvor den Alert Manager-Schlüssel entfernt haben:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents\McALSNMP

8. Starten Sie Windows NT-Explorer. Suchen Sie dann nach den folgenden Ordnern, und löschen Sie sie mitsamt ihrem Inhalt:

- C:\Programme\Network Associates\Tvd\GroupShield Exchange

  Dies ist das Standardinstallationsverzeichnis. Falls Sie während der “Installieren von GroupShield für Exchange“ auf Seite 34 festgelegt haben, GroupShield für Exchange in einem anderen Ordner zu installieren, suchen Sie nach diesem Ordner, und löschen Sie alle Programmdateien von GroupShield für Exchange.

- <Exchange Server-Verzeichnis>\Add-ins\NAISAdm

  <Exchange Server-Verzeichnis> ist das Verzeichnis, in dem Ihre Microsoft Exchange-Serversoftware installiert ist. Die spitzen Klammern dürfen Sie nicht eingeben.

9. Wechseln Sie zum Verzeichnis Network Associates im Verzeichnis \Programme\Gemeinsame Dateien, und löschen Sie alle Objekte, die nicht von anderen installierten McAfee-Virenschutzprodukten verwendet werden.

10. Um sich zu vergewissern, daß GroupShield für Exchange vollständig entfernt ist, führen Sie das Microsoft Windows Installer-Dienstprogramm CleanUp aus.

    Dieses Dienstprogramm erhalten Sie auf der Microsoft Support-Website. Suchen Sie dort nach dem Artikel **Q238413**. Downloaden Sie dieWindows NT-Version, **MSICUU.EXE**.

    http://support.microsoft.com/support/kb/articles/Q238/4/13.asp

11. Um GroupShield für Exchange v4.5 neu zu installieren, müssen Sie jetzt den Server neu starten und SETUP.EXE erneut ausführen. Führen Sie dann die in “Installieren von GroupShield für Exchange” aufgelisteten Schritte aus.

Scanvorgänge „bei Zugriff“ 3

GroupShield für Exchange bietet zwei grundlegende Virenscanmethoden: Scanvorgänge „bei Zugriff“ (sie werden in diesem Kapitel beschrieben) und Scanvorgänge „auf Anforderung“ (beschrieben unter “Scanvorgänge auf Anforderung”).

Die Registerkarte Bei Zugriff der Serververwaltungskonsole GroupShield-Eigenschaften besteht aus drei Abschnitten:

- Scanoptionen (siehe diese Seite)
- Bei Viruserkennung zu ergreifende Maßnahme Seite 65
- Anlagenblockierung, Seite 66.

Scanvorgänge bei Zugriff beziehen sich ausschließlich auf das Durchsuchen von E-Mail-Anlagen, die in einem Postfach oder in einem Öffentlichen Ordner auf dem Microsoft Exchange-Server eintreffen.

❑ **ANMERKUNG:** Bei einem Scanvorgang bei Zugriff wird der Nachrichtentext nicht gescannt.

Für den Fall, daß GroupShield für Exchange eine infizierte Anlage entdeckt, können Sie veranlassen, daß die Software versucht, den Virus zu entfernen oder die Anlage zu löschen oder sie an den von Ihnen zuvor festgelegten Quarantäneort zu verschieben.

❑ **ANMERKUNG:** Bei einem Scanvorgang bei Zugriff wird die E-Mail-Benachrichtigung über ein gefundenes Virus nur an den Administrator gesendet. Der Absender oder Empfänger enthält keine E-Mail, die ihn darüber informiert, daß die Anlage infiziert ist. Wenn die Anlage jedoch nicht gesäubert werden kann, entfernt sie GroupShield für Exchange aus der Nachricht und ersetzt sie durch eine Datei namens ALERT.TXT, die der ursprüngliche Empfänger erhält. Weitere Informationen über die Ersatzdatei ALERT.TXT finden Sie in Kapitel 5, „Benachrichtigungen und Alarmmeldungen.“.

Scanoptionen

Um die Scanoptionen für einen Scanvorgang bei Zugriff festzulegen, führen Sie folgende Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Bei Zugriff, um die Registerkarte Bei Zugriff anzuzeigen (Abbildung 3-1 auf Seite 62).

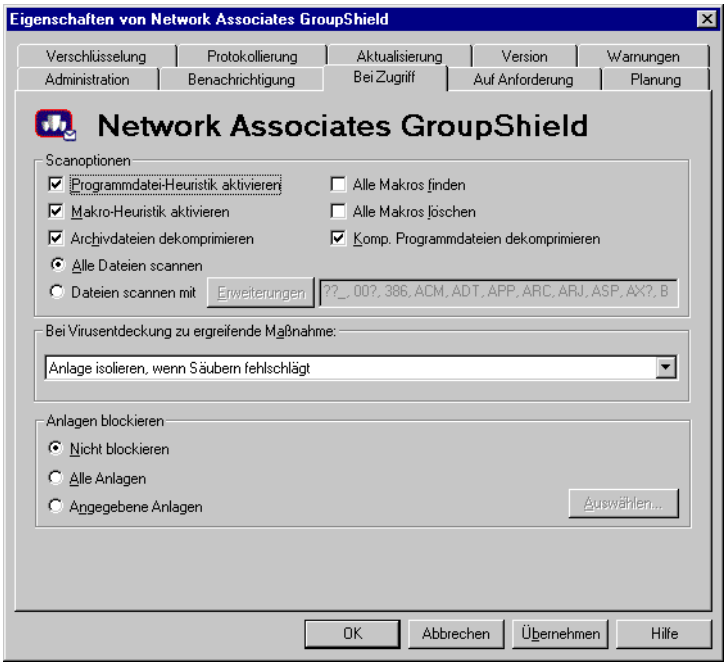


Abbildung 3-1. GroupShield-Eigenschaften - Registerkarte „Bei Zugriff“

2. Wählen Sie im Gruppenfeld **Scanoptionen** eine Kombination der folgenden Optionen, um GroupShield für Exchange anzugeben, welche Virensuchmethoden sie während eines Scanvorgangs bei Zugriff verwenden soll:

- **Programmdatei-Heuristik aktivieren** scannt Programmdateien und identifiziert mögliche neue Dateiviren.
- **Makro-Heuristik aktivieren** durchsucht die Dateien (z.B. Microsoft Word-, Microsoft Excel- und Microsoft Office-Dateien) nach Makros und identifiziert mögliche neue Makroviren.

- **Archivdateien dekomprimieren** scannt innerhalb von Dateiarchiven (wie z. B. .ZIP oder .LZH-Dateien). Wenn nur Dateien gescannt werden sollen, die bestimmte Erweiterungen haben, müssen Sie die erforderlichen Archivdateierweiterungen in die Liste der zu scannenden Dateierweiterungen aufnehmen.
- **Alle Dateien überprüfen** scannt sämtliche Anlagen.
- **Dateien mit Erweiterungen scannen** scannt standardmäßig alle Dateien. Führen Sie folgende Teilschritte aus, wenn Sie bestimmte Dateierweiterungen angeben möchten, die gescannt werden sollen:

  a. Sofern es noch nicht ausgewählt ist, aktivieren Sie das Optionsfeld **Scannen von Dateien mit**. Klicken Sie dann auf **Erweiterungen**.

  Das Dialogfeld Programmdateierweiterungen (Abbildung 3-2) zeigt alle Dateierweiterungen an, die GroupShield für Exchange scannt.

Abbildung 3-2. Registerkarte „Bei Zugriff“ - Dialogfeld Programmdateierweiterungen

In der Standardeinstellung scannt GroupShield für Exchange alle aufgelisteten Erweiterungen. McAfee empfiehlt, dass Sie zur Verbesserung der Scanleistung alle diejenigen Arten von Erweiterungen aus der Liste entfernen, die Sie bei Ihrer täglichen Arbeit üblicherweise nicht antreffen. Sie können jederzeit zu dieser Liste zurückkehren, um Erweiterungen bestimmter Dateitypen hinzuzufügen oder zu entfernen.

Im Dialogfeld Programmdateierweiterungen sind die folgenden Optionen verfügbar:

– Wenn Sie eine Dateierweiterung von dem Scanvorgang bei Zugriff ausschließen möchten, wählen Sie die Erweiterung aus und klicken auf **Löschen**.

– Wenn Sie eine neue Dateierweiterung hinzufügen möchten, klicken Sie auf **Hinzufügen** (Abbildung 3-3), geben den Namen der neuen Erweiterung in das Feld **Zu scannende Typen** ein und klicken auf **OK**, um die Erweiterung in die Liste aufzunehmen und zum Dialogfeld Programmdateierweiterungen zurückzukehren.

Abbildung 3-3. Dialogfeld Programmdateierweiterungen - Textfeld Typen scannen

– Wenn Sie zur GroupShield für Exchange-Originalliste der Dateierweiterungen zurückkehren möchten, klicken Sie auf **Zurück zu Standard**.

b. Klicken Sie auf **OK**, um zur Registerkarte Bei Zugriff zurückzukehren.

ANMERKUNG: McAfee empfiehlt, daß Sie die Standardliste der Dateierweiterungen für einen Scanvorgang bei Zugriff nicht ändern.

- **Nach allen Makros suchen** scannt speziell Anlagen, die Makros enthalten, und behandelt diese als Viren, die nicht gesäubert werden können. Die Anlage wird isoliert und der Administrator wird über die unternommene Aktion benachrichtigt.
- **Alle Makros löschen** kann nur in Kombination mit der Option **Nach allen Makros suchen** verwendet werden. Wählen Sie diese Kombination, wenn GroupShield für Exchange alle Makros finden und sie unabhängig davon, ob sie infiziert sind oder nicht, aus der Anlage entfernen soll.

ANMERKUNG: Jede Option der Kombinationsfelder Bei Viruserkennung zu ergreifende Maßnahme, bei der nicht versucht wird, eine infizierte Anlage zu säubern, kann nur dann ausgewählt werden, wenn die Optionen Nach allen Makros suchen und Alle Makros löschen weder auf der Registerkarte Bei Zugriff noch auf der Registerkarte Auf Anforderung aktiviert sind.

- **Kompr. Programmdateien dekomprimieren** scannt innerhalb komprimierten Dateien (z.B. Dateien, die mit PKLITE komprimiert wurden). Falls Sie nur Dateien mit ausgewählten Namenserweiterungen scannen, müssen Sie die erforderlichen Namenserweiterungen der komprimierten Dateien in die Liste der zu durchsuchenden Namenserweiterungen aufnehmen.

3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die SerververwaltungskonsoleGroupShield-Eigenschaftenschließenmöchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die SerververwaltungskonsoleGroupShield-Eigenschaftenschließenmöchten
- KlickenSieauf**Übernehmen**,wennSiedieÄnderungenspeichernmöchtenund dieSerververwaltungskonsoleGroupShield-Eigenschaftengeöffnetbleibensoll.

Festlegen der Aktionen zur Behandlung aufgespürter Viren

Um die Aktionen anzugeben, die GroupShield für Exchange beim Aufspüren einer infizierten Anlage durchführen soll, führen Sie die folgenden Schritte aus:

1. ÖffnenSiedieSerververwaltungskonsoleGroupShield-Eigenschaften,undklicken Sie auf die Registerkarte Bei Zugriff.
2. Klicken Sie in dem Kombinationsfeld Bei Viruserkennung zu ergreifende Maßnahme auf das Pfeilsymbol „Nach unten“, um eine Liste der möglichen Optionen einzublenden. Aktivieren Sie eine der folgenden Optionen:

- **Infektion protokollieren und weiter ohne Säuberung** legt im McAfee Log Manager einen Datensatz an, der darüber informiert, daß der Scanvorgang bei Zugriff einen Virus entdeckt hat. Außerdem wird der Administrator benachrichtigt. Allerdings veranlaßt diese Option keine Ausweichaktion zur Bekämpfung der Infektion.

> **ANMERKUNG:** McAfee empfiehlt, die Option Infektion protokollieren und weiter ohne Säuberung **NICHT** zu wählen.

- **Anlage isolieren, ohne Säuberung zu versuchen** sendet alle infizierten Anlagen an den Quarantäneort. Außerdem werden der Administrator und der ursprüngliche Adressat über die Aktion informiert.
- **Anlage isolieren, wenn Säuberung fehlschlug** versucht, die Anlage zu säubern. Ist dies erfolgreich, werden die Nachricht und ihre Anlage an den vorgesehenen Empfänger weitergeleitet, ohne diesen davon in Kenntnis zu setzen, daß die Anlage ursprünglich eine Virus enthielt. Andernfalls entfernt das Programm die Anlage aus der E-Mail-Nachricht und sendet sie an den Quarantäneort. Der vorgesehene Empfänger erhält also die Nachricht, aber die Anlage wird dabei durch eine Datei namens ALERT.TXT ersetzt.

- **Anlage löschen, wenn Säuberung fehlschlug** versucht, die Anlage zu säubern. Ist dies erfolgreich, werden die Nachricht und ihre Anlage an den vorgesehenen Empfänger weitergeleitet, und der Administrator erhält eine Benachrichtigung, die ihn über den enthaltenen Virus informiert. Ist dies nicht erfolgreich, wird die Anlage gelöscht und die Aktion im McAfee Log Manager protokolliert.
- **Infizierte Anlage löschen** versucht nicht, eine infizierte Anlage zu säubern oder zu isolieren. Die Anlage wird gelöscht, und diese Aktion wird im McAfee Log Manager protokolliert.

❑ **ANMERKUNG:** Um den Speicherort der Utility-Datenbank des Log Manager zu ändern und der Software die Protokollierung von Virusbenachrichtigungen bei Zugriff und auf Anforderung in der neuen Log Manager-Datenbank zu ermöglichen, müssen Sie den GroupShield für Exchange-Dienst neu starten. Entsprechende Anleitungen finden Sie in Kapitel 2, „Erste Schritte“.

---

3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll.

Blockieren von Anlagen bestimmten Typs

Mit dem Feld Anlagenblockierung können Sie GroupShield für Exchange angeben, welche Anlagentypen sofort isoliert werden sollen, bevor sie vom Scanner bei Zugriff durchsucht werden.

Um bestimmte Arten von Anlagen direkt an den Quarantäneort senden zu lassen, führen Sie folgende Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Bei Zugriff.
2. Aktivieren Sie im Feld **Anlagenblockierung** einen der folgenden Optionen, um GroupShield für Exchange anzugeben, welche Anlagen von Scanvorgängen bei Zugriff ausgeschlossen und sofort isoliert werden sollen:

- **Keine Blockierung** bewirkt, daß der Bei Zugriff-Scanvorgang alle Anlagen durchsucht, ohne sie aufgrund ihres Dateinamens oder –inhalts zu blockieren.
- Bei **Alle Anlagen** werden alle Anlagen, die in einem öffentlichen Ordner oder einem Postfach eingetroffen sind, sofort an den Quarantäneort gesendet.
- Bei **Angegebene Anlagen** werden Anlagen eines bestimmten Typs direkt an den Quarantäneort gesendet, bevor die jeweilige Anlage von dem Scanner bei Zugriff durchsucht wird. Außerdem kann diese Option Anlagen, die einen bestimmten Dateinamen oder eine bestimmte Größe haben, blockieren.

  Um Anlagen bestimmten Typs zu isolieren, führen Sie die folgenden Teilschritte aus:

  a. Aktivieren Sie im Feld Anlagenblockierung das Optionsfeld **Angegebene Anlagen**.

  b. Klicken Sie auf **Auswählen**.

  c. Verwenden Sie im Dialogfeld Blockieroptionen (Abbildung 3-4) das Feld Namensbasierte Optionen, um die Dateinamen oder Erweiterungstypen anzugeben, die sofort isoliert werden sollen.

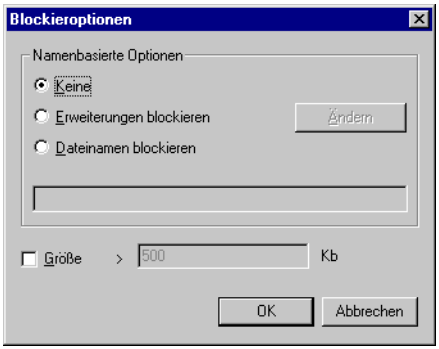


Abbildung 3-4. Registerkarte „Bei Zugriff“ - Dialogfeld „Blockieroptionen“

- **Keine** weist GroupShield für Exchange an, daß alle Erweiterungstypen und Dateinamen in einem Postfach oder öffentlichen Ordner abgelegt werden dürfen.
- **Erweiterungen blockieren** ermöglicht es Ihnen, die Erweiterungstypen auszuwählen, die von Scanvorgängen ausgeschlossen werden sollen.

  a. Klicken Sie auf **Erweiterungen blockieren** und dann auf **Ändern**, um das Dialogfeld Programmdateierweiterungen (siehe Abbildung 3-2 auf Seite 63) zu öffnen.

In der Standardeinstellung blockiert GroupShield für Exchange alle im Dialogfeld Programmdateierweiterungen aufgelisteten Arten von Anlagen. McAfee empfiehlt, daß Sie alle diejenigen Erweiterungstypen auswählen, die in Ihrer täglichen Arbeit am häufigsten auftreten und deshalb die größte Gefahr darstellen.

Die folgenden Optionen sind im Dialogfeld Programmdateierweiterungen verfügbar.

– Um GroupShield für Exchange daran zu hindern, Dateien mit einer bestimmten Namenserweiterung zu blockieren, markieren Sie die Erweiterung und klicken dann auf **Löschen**.

Alle Anlagen diesen Typs werden nun bei einem Scanvorgang „bei Zugriff“ berücksichtigt.

– Wenn ein Erweiterungstyp, den Sie blockieren möchten, noch nicht in der Liste enthalten ist, klicken Sie auf **Hinzufügen** und geben den Namen der Erweiterung in das Feld Erweiterungen hinzufügen ein (siehe Abbildung 3-3 auf Seite 64). Klicken Sie dann auf **OK**, um den Erweiterungstyp zur Liste hinzuzufügen.

– Wenn Sie zur GroupShield für Exchange-Originalliste der Dateierweiterungen zurückkehren möchten, klicken Sie auf **Zurück zu Standard**.

b. Klicken Sie auf **OK**, um zum Dialogfeld Blockieroptionen zurückzukehren.

❑ **ANMERKUNG:** Wenn eine Erweiterung, die blockiert werden soll, auch in der Liste Scanoptionen ausgewählt ist, erhält die Blockieraktion Vorrang, und die Anlage wird sofort isoliert.

- **Dateinamen blockieren** ermöglicht es Ihnen, Anlagen mit bestimmten Dateinamen direkt an den Quarantäneort zu senden. Um eine Anlage in Abhängigkeit von ihrem Dateinamen zu blockieren, führen Sie die folgenden Teilschritte aus:

  a. Klicken Sie auf **Dateinamen blockieren** und dann auf **Ändern**, um das Dialogfeld Programmdateierweiterungen (siehe Abbildung 3-5) zu öffnen.

Abbildung 3-5. Dialogfeld „Blockieroptionen“ - Liste „Programmdateien“

b. Klicken Sie auf **Hinzufügen**, und geben Sie in das Textfeld Dateiname hinzufügen (Abbildung 3-6) den Dateinamen ein, der blockiert werden soll.

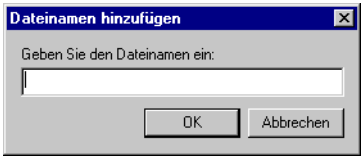


Abbildung 3-6. Liste „Programmdateien“ - Textfeld „Dateiname hinzufügen“

Um einen Dateinamen aus der Liste zu entfernen, markieren Sie ihn und klicken auf **Löschen**.

WICHTIG: Damit eine Anlage nach dem Dateinamen blockiert wird, müssen Sie den vollständigen Dateinamen samt seiner Erweiterung eingeben, also z.B. EICAR.COM.

---

c. Klicken Sie auf **OK**, damit der Dateiname in die Liste Programmdateien aufgenommen wird, und klicken Sie dann erneut auf **OK**, um zum Dialogfeld Blockieroptionen zurückzukehren.

d. Aktivieren Sie das Kontrollkästchen **Größe**, damit GroupShield für Exchange Anlagen blockiert, deren Größe einen von Ihnen angegebenen Wert übersteigt. Geben Sie den für die Größe gewünschten Wert in KB ein.

In der Standardeinstellung scannt GroupShield für Exchange Anlagen beliebiger Größe.

e. Klicken Sie auf **OK**, um zur Registerkarte Bei Zugriff zurückzukehren.

3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll.

TIP: Falls auf demselben Server auch ein McAfee Desktop-Virenschutzprogramm (beispielsweise NetShield für Windows NT) installiert ist, empfiehlt McAfee, das Verzeichnis **qtinewrk** von den Scanvorgängen des Desktop-Scanners auszuschließen. Wenn Sie das unterlassen, informiert Sie die NetShield-Software darüber, daß das Verzeichnis infizierte Objekte enthält. In Ihrer Dokumentation wird beschrieben, wie Verzeichnisse von Scanvorgängen ausgeschlossen werden.

Scanvorgänge auf Anforderung

4

GroupShield für Exchange bietet zwei grundlegende Virenscanmethoden: Scanvorgänge auf Anforderung (sie werden in diesem Kapitel beschrieben) und Scanvorgänge bei Zugriff (beschrieben unter Kapitel 3, „Scanvorgänge „bei Zugriff““).

Bei einem Scanvorgang auf Anforderung wird auf Anforderung oder in voreingestellten Intervallen nach Viren gesucht. Wenn ein Virus erkannt wird, kann GroupShield für Exchange versuchen, das Virus zu säubern oder die infizierte(n) Datei(en) an einen Quarantäneort zu verschieben.

Je nach dem, wie anfällig Ihr E-Mail-System für Virusinfektionen ist, sollten Sie einen Scan auf Anforderung bis zu einmal täglich durchführen. Wählen Sie eine Zeit, zu der der E-Mail-Verkehr gering ist, um Ihren Mail-Server so wenig wie möglich zu belasten. Um sicherzustellen, daß ihre Virenschutz-Software auf dem neuesten Stand ist, müssen Sie die McAfee-Virusdefinitionsdateien (.DAT) regelmäßig aktualisieren. In Kapitel 7, „Automatische Aktualisierung der .DAT-Dateien“ finden Sie diesbezügliche Informationen.

Dieses Kapitel enthält die folgenden Abschnitte:

- “Auswahl der zu scannenden Objekte“ auf Seite 72
- “Scanoptionen“ auf Seite 76
- “GroupShield für Exchange-Aktionen bei Viruserkennung“ auf Seite 79
- “Scannen neuer oder geänderter E-Mail-Anlagen“ auf Seite 81
- “Bericht auf Anforderung“ auf Seite 83
- “Planen von Scanvorgängen auf Anforderung“ auf Seite 85
- “Konsole für das Scannen auf Anforderung - Einführung“ auf Seite 89
- “Durchführen eines Scanvorgangs auf Anforderung über die Befehlszeile“ auf Seite 99.

Konfigurieren von Scanvorgängen auf Anforderung

Auswahl der zu scannenden Objekte

Um GroupShield für Exchange mitzuteilen, welche öffentlichen Ordner und Postfächer in den Scanvorgang auf Anforderung aufzunehmen sind, führen Sie folgende Schritte durch:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Auf Anforderung, um die Registerkarte Auf Anforderung anzuzeigen (Abbildung4-1).

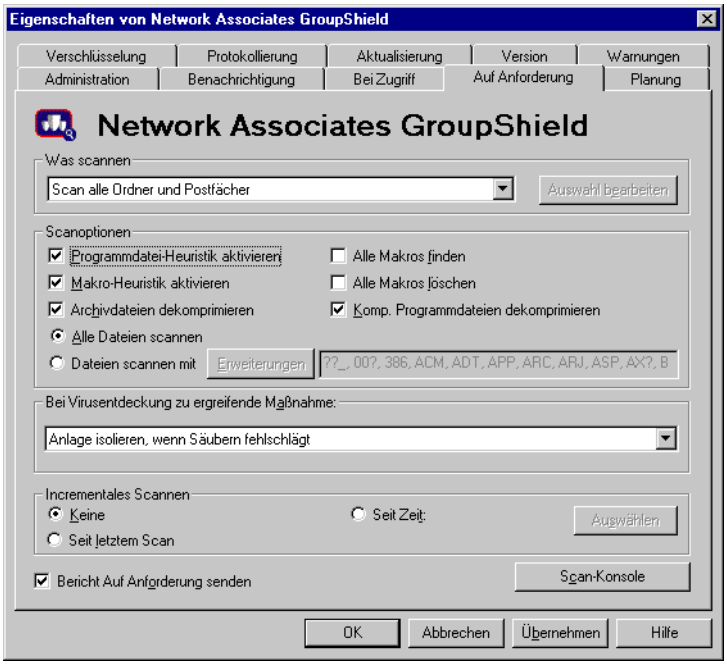


Abbildung 4-1. GroupShield-Eigenschaften - Auf Anforderung (Registerkarte)

2. Wählen Sie im Feld Was scannen eine der folgenden Optionen aus, um GroupShield für Exchange mitzuteilen, welche Ordner und Postfächer es scannen soll:

- **ALLE Ordner und Postfächer scannen** ist die Standardoption und scannt auf dem GroupShield für Exchange-Server alle öffentlichen Ordner und alle Postfächer.
- **Alle Ordner und Postfächer MIT AUSNAHME der ausgewählten scannen** gibt GroupShield für Exchange die Objekte an, die vom Scanvorgang auf Anforderung auszuschließen sind.

WICHTIG: Sie können nicht mehr als 450 Postfächer oder öffentliche Ordner ausschließen.

Um bestimmte Ordner und Postfächer vom Scanvorgang auszuschließen, führen Sie diese Teilschritte aus:

a. Wählen Sie im Feld Was scannen die Option **Alle Ordner und Postfächer MIT AUSNAHME der ausgewählten scannen**.

b. Klicken Sie auf **Auswahl bearbeiten**.

c. Klicken Sie im Dialogfeld Liste Auswahl (Abbildung4-2) auf **Ordner hinzufügen**, um ausgewählte öffentliche Ordner vom Scanvorgang auf Anforderung auszuschließen.

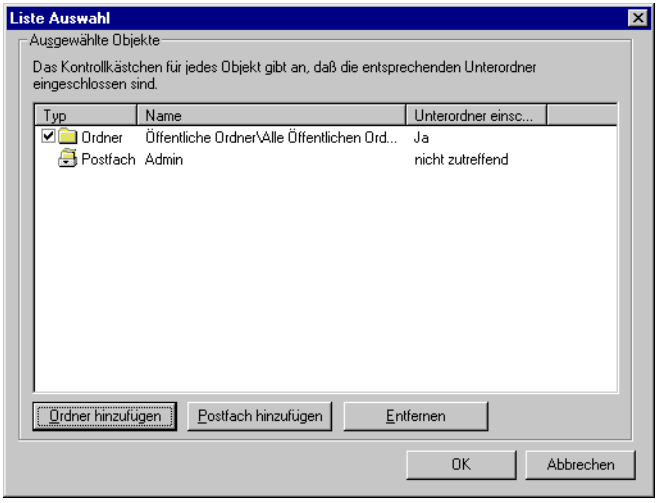


Abbildung 4-2. Auf Anforderung (Registerkarte) - Dialogfeld Liste Auswahl

d. Bewegen Sie sich im Dialogfeld Ordner auswählen (Abbildung4-3) zu dem gewünschten öffentlichen Ordner, wählen Sie diesen aus, und klicken Sie auf **OK**, um ihn zu Liste Auswahl hinzuzufügen.

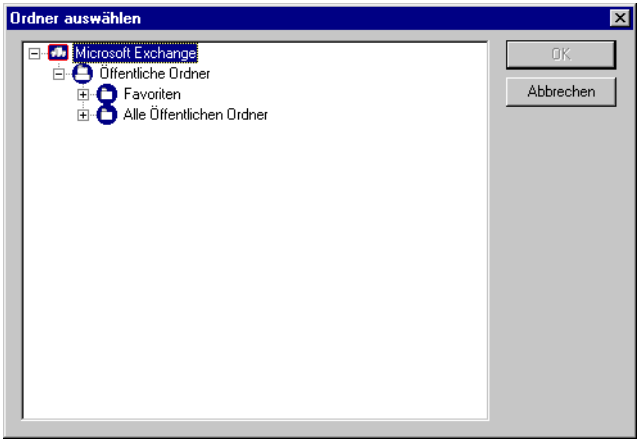


Abbildung 4-3. Dialogfeld Liste Auswahl - Feld Ordner auswählen

ANMERKUNG: Das Kontrollkästchen in der Spalte **Typ** im Dialogfeld Liste Auswahl gibt an, daß die Unterordner ebenfalls vom Scannen ausgenommen werden.

e. Wiederholen Sie die Schritte c) und d) so oft wie nötig.

f. Um bestimmte Postfächer vom Scanvorgang auf Anforderung auszuschließen, klicken Sie im Dialogfeld Liste Auswahl auf **Postfach hinzufügen**.

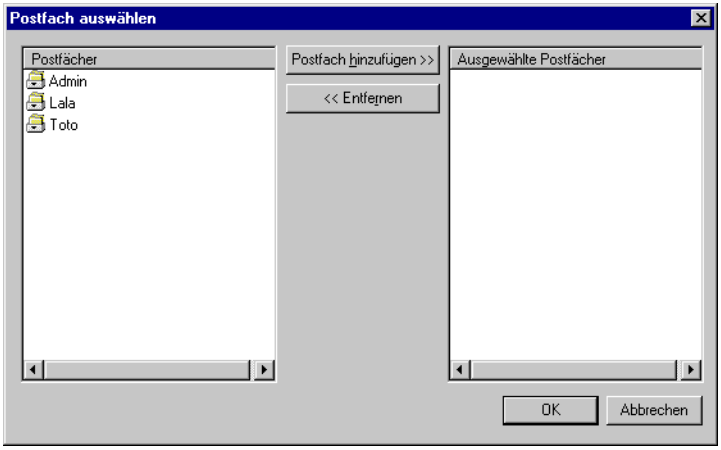


Abbildung 4-4. Dialogfeld Liste Auswahl - Feld Postfach auswählen

g. Wählen Sie in der Spalte Postfächer des Dialogfelds Postfach auswählen (Abbildung 4-4 auf Seite 74) die Postfächer aus, die Sie in den Scanvorgang zu auf Anforderung aufnehmen möchten, und klicken Sie auf **Postfach hinzufügen>>**, um das Objekt in die Spalte Ausgewählte Postfächer zu verschieben.

h. Klicken Sie auf **OK**, um zum Dialogfeld Liste Auswahl zurückzukehren, und klicken Sie dann nochmals auf **OK**, um zur Registerkarte Auf Anforderung zurückzukehren.

- Die Option **AUSGEWÄLTE Ordner und Postfächer scannen** legt für GroupShield für Exchange fest, welche Ordner und Postfächer im Einzelnen bei einem Scanvorgang auf Anforderung einbezogen werden sollen.

  Um bestimmte Ordner und Postfächer zu scannen, führen Sie diese Teilschritte aus:

  a. Klicken Sie im Feld Was scannen auf **AUSGEWÄHLTE Ordner und Postfächer scannen**.

  b. Klicken Sie auf **Auswahl bearbeiten**.

  c. Klicken Sie im Dialogfeld Liste Auswahl (Abbildung 4-2 auf Seite 73) auf **Ordner hinzufügen**, um ausgewählte öffentliche Ordner zum Scanvorgang auf Anforderung hinzuzufügen.

  d. Bewegen Sie sich im Dialogfeld Ordner auswählen (Abbildung 4-3 auf Seite 74) zu dem gewünschten öffentlichen Ordner, wählen Sie diesen aus, und klicken Sie auf **OK**, um ihn zu Liste Auswahl hinzuzufügen.

     Das Kontrollkästchen in der Spalte **Typ**gibt an, daß die Unterordner ebenfalls in den Scanvorgang auf Anforderung aufgenommen werden.

  e. Wiederholen Sie die Schritte c und d so oft, wie nötig.

  f. Um bestimmte Postfächer in den Scanvorgang aufzunehmen, wählen Sie im Dialogfeld Liste Auswahl die Option **Postfach hinzufügen**.

  g. Wählen Sie in der Spalte Postfächer des Dialogfelds Postfach auswählen (Abbildung 4-4 auf Seite 74) die Postfächer aus, die Sie vom Scanvorgang auf Anforderung ausschließen möchten, und klicken Sie auf **Postfach hinzufügen>>**, um sie in die Spalte Ausgewählte Postfächer zu verschieben.

  h. Klicken Sie auf **OK**, um zum Dialogfeld Liste Auswahl zurückzukehren, und klicken Sie dann nochmals auf **OK**, um zur Registerkarte Auf Anforderung zurückzukehren.

3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Scankonsole**, um zur Konsole für das Scannen auf Anforderung zu gelangen. Anweisungen zur Verwendung der Konsole für das Scannen auf Anforderung finden Sie in “Konsole für das Scannen auf Anforderung - Einführung“ auf Seite 89.
- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll.

  Wählen Sie eine andere Registerkarte, oder klicken Sie auf **Scankonsole**, um die Konsole für das Scannen auf Anforderung zu öffnen und den Scanvorgang zu starten.

  Die Verwendung der Konsole für das Scannen auf Anforderung wird auf Seite 89 beschrieben.

Scanoptionen

Ein Scanvorgang auf Anforderung kann im Hauptteil von E-Mail-Nachrichten nach in VBScript geschriebenen eingebetteten Viren suchen. Ein kürzlich entdecktes Virus namens VBS/BUBBLEBOY kann VBScript-Code im Hauptteil einer E-Mail-Nachricht, die mit HTML-Tags formatiert ist, verbergen. Bestimmte Windows- und Internet Explorer-Konfigurationen lassen es zu, daß das eingebettete Skript ausgeführt wird, sobald es in der Microsoft Outlook Express-Vorschau angezeigt wird oder der Nachrichtenempfänger die E-Mail-Nachricht in Microsoft Outlook öffnet.

Führen Sie folgende Teilschritte aus, wenn Sie bestimmte Dateierweiterungen angeben möchten, die gescannt werden sollen:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Auf Anforderung.
2. Wählen Sie im Feld Scanoptionen eine Kombination der folgenden Optionen, um GroupShield für Exchange mitzuteilen, welche Virensuchmethoden sie während eines Scanvorgangs auf Anforderung verwenden soll:

- **Programmdatei-Heuristik aktivieren** scannt Programmdateien und identifiziert mögliche neue Dateiviren
- **Makro-Heuristik aktivieren** durchsucht die Anlagen (z. B. Microsoft Word-, Microsoft Excel- und Microsoft Office-Dateien) nach Makros und identifiziert mögliche neue Makroviren
- **Archivdateien dekomprimieren** scannt innerhalb von Dateiarchiven (wie z. B. .ZIP oder .LZH-Dateien). Wenn nur Dateien gescannt werden sollen, die bestimmte (Namens-)Erweiterungen haben, müssen Sie die erforderlichen Archivdateierweiterungen in die Liste der von der Software zu scannenden Dateierweiterungen aufnehmen
- **Alle Dateien überprüfen** scannt sämtliche Anlagen
- **Dateien mit Erweiterungen scannen** scannt standardmäßig alle Dateien. Um GroupShield für Exchange mitzuteilen, welche Erweiterungen in einen Scanvorgang auf Anforderung aufzunehmen sind, führen Sie diese Teilschritte durch:

  a. Sofern es noch nicht aktiviert ist, aktivieren Sie das Optionsfeld **Scannen von Dateien mit**. Klicken Sie dann auf **Erweiterungen**, um das Dialogfeld Programmdateierweiterungen anzuzeigen (Abbildung4-5).

Abbildung 4-5. Auf Anforderung (Registerkarte) - Dialogfeld Programmdateierweiterungen

Das Dialogfeld Programmdateierweiterungen zeigt alle Dateierweiterungen an, die GroupShield für Exchange scannt. Folgende Optionen sind verfügbar:

– Damit GroupShield für Exchange eine neue Dateierweiterungen in einen Scanvorgang auf Anforderung aufnimmt, klicken Sie auf **Hinzufügen**, um das Feld Typen scannen einzublenden (Abbildung 4-6 auf Seite 78).

Geben Sie den Namen der neuen Erweiterung ein, und klicken Sie auf **OK**, um zum Dialogfeld Programmdateierweiterungen zurückzukehren und sie in der Liste zu registrieren.

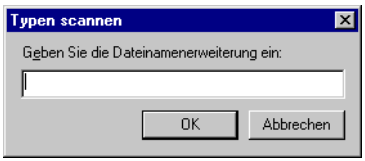


Abbildung 4-6. Dialogfeld Programmdateierweiterungen - Textfeld Typen scannen

– Um GroupShield für Exchange mitzuteilen, daß sie bei einem Scanvorgang auf Anforderung eine bestimmte Dateierweiterung nicht scannen soll, markieren Sie sie, und klicken Sie auf **Löschen**.

– Um wieder die Originalliste der Dateierweiterungen, die GroupShield für Exchange bei einem Scanvorgang auf Anforderung scannt, herzustellen, klicken Sie auf **Standardeinstellung**.

b. Klicken Sie auf **OK**, um zur Registerkarte Auf Anforderung zurückzukehren.

ANMERKUNG: Wenn beim Scannen ein HTML- oder VBScript-Virus in einer E-Mail-Nachricht entdeckt wird, werden die gesamte Nachricht und alle darin enthaltenen Anlagen isoliert, auch wenn nur die Option **Anlage isolieren** auf der Registerkarte **Auf Anforderung** ausgewählt ist. Die Anwendung verschiebt die infizierten Nachricht in die Quarantänedatenbank oder in das Quarantäneverzeichnis.

- **Nach allen Makros suchen** scannt speziell Anlagen, die Makros enthalten, und behandelt diese als Viren, die nicht gesäubert werden können. Die Anlage wird isoliert und der Administrator über die Aktion benachrichtigt.
- **Alle Makros löschen** kann nur zusammen mit der Option Nach allen Makros suchen verwendet werden. Sie entdeckt alle Makros und löscht diese unabhängig davon, ob sie infiziert sind oder nicht.
- **Kompr. Programmdateien dekomprimieren** scannt innerhalb komprimierter Dateien (z. B. Dateien, die mit PKLITE komprimiert wurden). Wenn nur Dateien gescannt werden sollen, die bestimmte Erweiterungen haben, müssen Sie die erforderlichen Erweiterungen für komprimierte Dateien in die Liste der zu scannenden Dateierweiterungen aufnehmen.

ANMERKUNG: Um den Speicherort der Utility-Datenbank des Log Manager zu ändern und der Software die Protokollierung von Virusbenachrichtigungen bei Zugriff und auf Anforderung in der neuen Log Manager-Datenbank zu ermöglichen, müssen Sie den GroupShield für Exchange-Dienst neu starten. Entsprechende Anleitungen finden Sie in Kapitel 2, „Erste Schritte“.

3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Scankonsole**, um zur Konsole für das Scannen auf Anforderung zu gelangen. Anweisungen zur Verwendung der Konsole für das Scannen auf Anforderung finden Sie in “Konsole für das Scannen auf Anforderung - Einführung“ auf Seite 89
- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll.

  Wählen Sie eine andere Registerkarte, oder klicken Sie auf **Scankonsole**, um die Konsole für das Scannen auf Anforderung zu öffnen und den Scanvorgang zu starten. Das Starten des Scanvorgangs mit Hilfe der Konsole für das Scannen auf Anforderung wird auf Seite 89 beschrieben.

GroupShield für Exchange-Aktionen bei Viruserkennung

Um die Aktionen anzugeben, welche GroupShield für Exchange beim Aufspüren einer infizierten E-Mail-Nachricht oder Anlage durchführen soll, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Auf Anforderung.
2. Wählen Sie im Feld Bei Viruserkennung zu ergreifende Maßnahme eine der folgenden Optionen aus, um GroupShield für Exchange mitzuteilen, wie sie infizierte Anlagen während eines Scanvorgangs behandeln soll:

- **Infektion protokollieren und weiter ohne Säuberung** legt im McAfee Log Manager einen Datensatz an, der darüber informiert, daß der Scanvorgang auf Anforderung ein Virus entdeckt hat. Außerdem wird der Administrator benachrichtigt. Allerdings veranlaßt diese Option keine Ausweichaktion zur Bekämpfung der Infektion.

  ANMERKUNG: McAfee empfiehlt, die Option Infektion protokollieren und weiter ohne Säuberung **NICHT** zu wählen.

- **Anlage isolieren, ohne Säuberung zu versuchen** sendet alle infizierten Anlagen an den Quarantäneort.
- **Nachricht isolieren, ohne Säuberung zu versuchen** sendet alle infizierten Nachrichten und ihre Anlagen an den Quarantäneort.
- **Anlage isolieren, wenn Säuberung fehlschlug** versucht, die Anlage zu säubern. Ist dies erfolgreich, werden die Nachricht und ihre Anlage an den vorgesehenen Empfänger weitergeleitet. Ist dies nicht erfolgreich, wird die Anlage isoliert. Ist dies erfolgreich, wird der vorgesehene Empfänger nicht benachrichtigt, daß die Anlage einen Virus enthielt.
- **Nachricht isolieren, wenn Säuberung fehlschlug** versucht, die Anlage zu säubern. Ist dies erfolgreich, werden die Nachricht und die Anlage an den vorgesehenen Empfänger weitergeleitet. Hat der Versuch keinen Erfolg, erfolgt eine Isolierung der Anlage UND der Nachricht.
- **Anlage löschen, wenn Säuberung fehlschlug** versucht, die Anlage zu säubern. Ist dies erfolgreich, werden die Nachricht und die Anlage an den vorgesehenen Empfänger weitergeleitet. Ist dies nicht erfolgreich, wird die Anlage gelöscht und die Aktion im McAfee Log Manager protokolliert.
- **Nachricht löschen, wenn Säuberung fehlschlug** versucht, die Anlage zu säubern. Ist dies erfolgreich, werden die Nachricht und die Anlage an den vorgesehenen Empfänger weitergeleitet. Kann die Anlage nicht gesäubert werden, wird die gesamte Nachricht gelöscht und diese Aktion durch McAfee Log Manager protokolliert.
- **Infizierte Anlage löschen** versucht nicht, eine infizierte Anlage zu säubern oder zu isolieren. Die Anlage wird gelöscht, und diese Aktion wird im McAfee Log Manager protokolliert.
- **Nachricht löschen, ohne Säuberung zu versuchen** macht keinen Versuch, eine infizierte Anlage zu säubern oder zu isolieren. Die gesamte Nachricht wird unmittelbar gelöscht und diese Aktion im McAfee Log Manager protokolliert.

ANMERKUNG: Wenn GroupShield für Exchange eine Anlage löscht, wird die Anlage durch die ALERT.TXT-Nachricht ersetzt.

3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Scankonsole**, um zur Konsole für das Scannen auf Anforderung zu gelangen. Anweisungen zur Verwendung der Konsole für das Scannen auf Anforderung finden Sie in "Konsole für das Scannen auf Anforderung - Einführung" auf Seite 89.
- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll.

Scannen neuer oder geänderter E-Mail-Anlagen

Je nach Größe Ihrer Organisation und dem Risiko von Virusinfektionen sollten Sie einen Scan auf Anforderung bis zu einmal täglich durchführen. Häufige Scans auf Anforderung können jedoch Ihre Microsoft Exchange-Server stark belasten. Um das Problem der starken Belastung zu verringern, können Sie mit GroupShield für Exchange einen inkrementellen Scanvorgang konfigurieren, der sich auf Dateien konzentriert, die im Postfach oder öffentlichen Ordner angekommen sind oder sich geändert haben. Dabei haben Sie die Wahl zwischen diesen Zeitpunkten:

- seit dem letzten Scanvorgang
- seit der von Ihnen angegebenen Zeit.

Um das inkrementelle Scanfeature zu aktivieren, führen Sie folgende Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Auf Anforderung.
2. Wählen Sie im Feld Inkrementelles Scannen eine der folgenden Optionen, damit GroupShield für Exchange nur Nachrichten scannt, die sich seit dem letzten Scan auf Anforderung oder seit dem von Ihnen angegebenen Zeitpunkt und Datum geändert haben:

- **Keiner** ist die Standardoption, wenn Sie GroupShield für Exchange installieren. Alle Nachrichten und Anlagen in allen öffentlichen Ordnern und Postfächer werden gescannt, unabhängig davon, ob sie bereits gescannt und für sauber befunden wurden.
- **Seit dem letzten Scanvorgang** scannt nur die Nachrichten und Anlagen, die sich seit dem letzten Scanvorgang geändert haben.
- **Seit Zeitpunkt** scannt nur die Nachrichten und Anlagen, die sich seit der angegebenen Zeit geändert haben. Um dieses Feature zu verwenden, führen Sie die folgenden Teilschritte aus:

  a. Klicken Sie im Feld Inkrementelles Scannen auf **Seit Zeitpunkt**, und klicken Sie dann auf **Auswählen**.

  b. Geben Sie im Dialogfeld Zeitpunkt angeben (Abbildung 4-7 auf Seite 82) den Zeitpunkt (Datum und Uhrzeit) an, auf den der aktuelle Scanvorgang Auf Anforderung seine Ergebnisse beziehen soll.

Abbildung 4-7. Registerkarte Auf Anforderung - Dialogfeld Zeitpunkt angeben

  c. Klicken Sie auf **OK**, um zur Registerkarte Auf Anforderung zurückzukehren.

3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Scankonsole**, um zur Konsole für das Scannen auf Anforderung zu gelangen. Anweisungen zur Verwendung der Konsole für das Scannen auf Anforderung finden Sie in “Konsole für das Scannen auf Anforderung - Einführung“ auf Seite 89.
- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll.

Wählen Sie eine andere Registerkarte, oder klicken Sie auf **Scankonsole**, um die Konsole für das Scannen auf Anforderung zu öffnen und den Scanvorgang zu starten.

Die Verwendung der Konsole für das Scannen auf Anforderung wird auf Seite 89 beschrieben.

Bericht auf Anforderung

GroupShield für Exchange sendet auf Wunsch einen Bericht an die auf der Registerkarte Administration aufgelisteten Administratoren, der detaillierte Ergebnisse eines Scanvorgangs auf Anforderung enthält. Verwenden Sie diesen Bericht, um die Virenscanstatistiken von GroupShield für Exchange zu analysieren oder zu archivieren.

Der Bericht gibt den Administratoren folgende Informationen:

- Welcher Microsoft Exchange-Server gescannt wurde
- Wie viele Nachrichten und Anlagen gescannt wurden
- Wann der Scanvorgang ausgeführt wurde
- Um wieviel Uhr der Scanvorgang gestartet bzw. beendet wurde
- Wie viele Nachrichten infiziert waren
- Wie viele Nachrichten isoliert wurden
- Wie viele Nachrichten gesäubert wurden

Um den Bericht auf Anforderung zu aktivieren, führen Sie diese Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Auf Anforderung.
2. Aktivieren Sie das Kontrollkästchen **Bericht auf Anforderung senden** im unteren Teil der Registerkarte.

   Sie können GroupShield für Exchange veranlassen, während eines Scanvorgangs auf Anforderung den Absender und den ursprünglichen Empfänger einer infizierten Nachricht über die Entdeckung eines Virus zu benachrichtigen und ihnen mitzuteilen, welche Maßnahme dagegen getroffen wurde. Siehe Kapitel 5, „Benachrichtigungen und Alarmmeldungen“.
3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Scankonsole**, um zur Konsole für das Scannen auf Anforderung zu gelangen. Anweisungen zur Verwendung der Konsole für das Scannen auf Anforderung finden Sie in “Konsole für das Scannen auf Anforderung - Einführung“ auf Seite 89

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten, oder den Scanvorgang zu starten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll.

❑ **ANMERKUNG:** Unter "Auswählen von Administratorpostfächern für den Empfang von Benachrichtigungen" auf Seite 113 erfahren Sie, wie Sie Administratoren, die diesen Bericht erhalten sollen, zur Liste hinzufügen oder von ihr entfernen.

Um den Auf Anforderung-Bericht nach einem Scanvorgang anzuzeigen, führen Sie diese Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Auf Anforderung.
2. Falls noch nicht geschehen, aktivieren Sie das Kontrollkästchen **Bericht auf Anforderung senden**.
3. Konfigurieren Sie nun einen Scanvorgang. Die verfügbaren Optionen werden unter "Konfigurieren von Scanvorgängen auf Anforderung" auf Seite 72 beschrieben.
4. Klicken Sie auf **Scankonsole**, um das Dienstprogramm Konsole für das Scannen auf Anforderung zu öffnen.
5. Folgen Sie den Anweisungen in "Verwenden der Konsole für das Scannen auf Anforderung" auf Seite 94, um den Scanvorgang zu starten.
6. Wenn der Scanvorgang abgeschlossen ist, öffnen Sie Ihre E-Mail-Clientssoftware und doppelklicken zum Öffnen des Berichts im Posteingang auf die Nachricht mit der folgenden Betreffzeile (Abbildung4-8):

   ```
   Network Associates GroupShield für Exchange - Bericht über Scan auf Anforderung
   ```

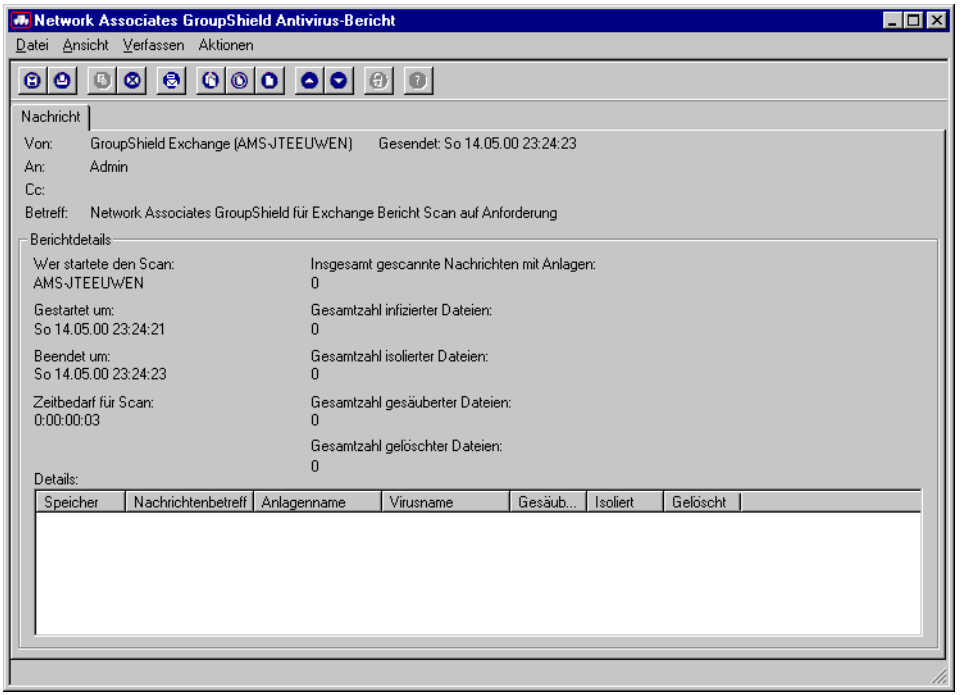


Abbildung 4-8. Virenschutzbericht von GroupShield für Exchange

> **ANMERKUNG:** Ein Bericht über einen Scan auf Anforderung kann auch nach einem geplanten Scanvorgang gesendet werden. Aktivieren Sie das Kontrollkästchen **Bericht auf Anforderung senden** auf der Registerkarte Einstellungen Scan auf Anforderung.

Planen von Scanvorgängen auf Anforderung

Um den Schutz von GroupShield für Exchange gegen Virusangriffe zu erhöhen, sollten Sie zukünftige einzelne oder regelmäßige Scanvorgänge konfigurieren. Ein geplanter Scanvorgang führt die gleichen Scanfunktionen aus wie ein Auf Anforderung-Scanvorgang. So können Sie sicherstellen, daß wichtige Scanvorgänge erfolgen, wenn die Microsoft Exchange-Server nicht viel zu tun haben oder Sie nicht im Büro sind.

> **ANMERKUNG:** Für den Fall, daß ein Vorgang auf Anforderung gerade ausgeführt wird, wenn ein zeitlich geplanter Scanvorgang startet, führt GroupShield für Exchange die beiden Scanvorgänge gleichzeitig aus.

Führen Sie folgende Schritte aus, um einen neuen zeitlich geplanten Scanvorgang hinzuzufügen:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Zeitplanung, um die Registerkarte Zeitplanung anzuzeigen (Abbildung4-9).

Abbildung 4-9 GroupShield-Eigenschaften - Registerkarte Planung

2. Klicken Sie auf **Ereignis hinzufügen**, damit das Dialogfeld Scan auf Anforderung planen angezeigt wird (Abbildung4-10).

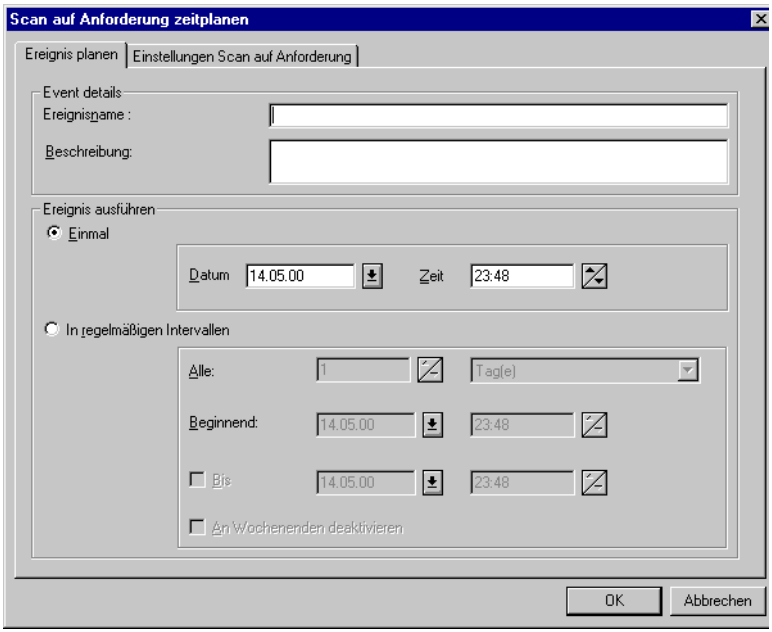


Abbildung 4-10. Planung (Registerkarte) - Dialogfeld Scan auf Anforderung planen

3. Geben Sie in das Feld Ereignisdetails einen eindeutigen Ereignisnamen ein. Geben Sie bei Bedarf eine Beschreibung des Ereignisses ein.

4. Aktivieren Sie im Feld Ereignis ausführen eine der folgenden Optionen, und führen Sie zugehörigen Schritte aus:

- **Einmal**, damit das Ereignis an Datum X zu Uhrzeit X auftritt. Wenn ein geplanter Scanvorgang, für den angegeben ist, daß er einmal auftreten soll, beendet wurde, wird das Ereignis aus der Liste Zeitgeplante Scans entfernt.

    a. Geben Sie das **Datum** an, an dem der Scanvorgang ausgeführt werden soll.

    b. Geben Sie mit den Pfeilen von **Zeit** den Zeitpunkt an, zu dem der Scanvorgang ausgeführt werden soll. Die Zeit muß auf 24-Stunden-Basis angegeben werden.

- **Zu regelmäßigen Intervallen**

  a. Verwenden Sie den Eintrag **Alle** des Kombinationsfelds, um anzugeben, wie oft der Scanvorgang ausgeführt werden soll. Geben Sie dann im Kombinationsfeld daneben die Zeitspanne an, die zwischen zwei Scanvorgängen liegen soll. Wählen Sie aus folgenden Optionen:

  – Stunde(n)

  – Tag(e)

  – Woche(n)

  – Monat(e)

  b. Teilen Sie GroupShield für Exchange dann Datum und Uhrzeit mit, wann die Scanvorgänge starten sollen.

  c. Wenn Sie einen Endtermin für einen regelmäßigen Scanvorgang angeben möchten, aktivieren Sie das Kontrollkästchen **Bis** und geben das Datum und die Uhrzeit für das letzte Ereignis ein.

  Wenn GroupShield für Exchange samstags und sonntags keine Scanvorgänge ausführen soll, aktivieren Sie das Kontrollkästchen **An Wochenenden deaktivieren**.

5. Wählen Sie die Registerkarte Einstellungen Scan auf Anforderung (Abbildung4-11).

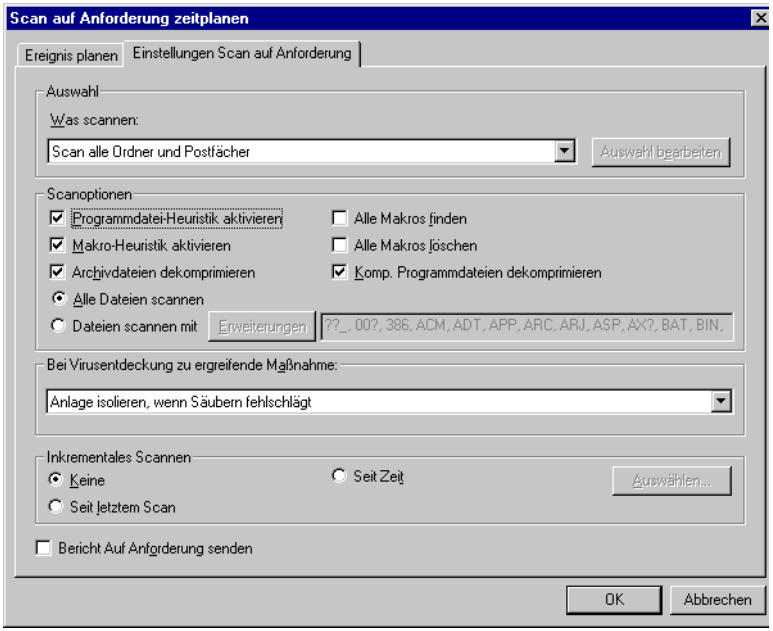


Abbildung 4-11. Registerkarte Einstellungen Scan auf Anforderung

Die Verwendung der Features und Funktionen auf der Registerkarte Einstellungen Scan auf Anforderung wird in den folgenden Abschnitten beschrieben:

- “Auswahl der zu scannenden Objekte“ auf Seite 72.
- “Scanoptionen“ auf Seite 76.
- “GroupShield für Exchange-Aktionen bei Viruserkennung“ auf Seite 79.
- “Scannen neuer oder geänderter E-Mail-Anlagen“ auf Seite 81.
- “Bericht auf Anforderung“ auf Seite 83.

6. Klicken Sie auf **OK**, um zur Registerkarte Planung zurückzukehren. Das hinzugefügte Ereignis wird in der Liste Zeitgeplante Scans angezeigt und zur angegebenen Zeit aktiviert.
7. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll. Klicken Sie auf eine andere Registerkarte.

  Die Verwendung der Konsole für das Scannen auf Anforderung wird auf Seite 89 beschrieben.

Ergänzende Planungsinformationen

- Wenn Sie ein vorhandenes Ereignis ändern möchten, wählen Sie es in der Liste **Zeitgeplante Scans** aus und klicken auf **Ereignis modifizieren**.
- Wenn Sie ein vorhandenes Ereignis entfernen möchten, wählen Sie es in der Liste **Zeitgeplante Scans** aus und klicken auf **Entfernen**.
- Wenn Sie feststellen möchten, ob ein zeitlich geplantes Ereignis aktiv ist, klicken Sie auf **Status aktualisieren**.

Konsole für das Scannen auf Anforderung - Einführung

Die Konsole zeichnet sich vor allem dadurch aus, daß

- sie für das Scannen des lokalen wie auch eines Remote-Computers konfiguriert werden kann.
- sie es ermöglicht, einen Scanvorgang zu starten, die Konsole zu schließen, sie anschließend erneut zu öffnen und eine Verbindung mit dem ablaufenden Scanvorgang herzustellen.
- sie einen Scanvorgang auf Anforderung gleichzeitig auch als geplanten Scanvorgang durchführen kann.

Die Konsole teilt mit, wie viele Viren in jedem Informationsspeicher auf dem Microsoft Exchange-Server gefunden, isoliert, gesäubert und gelöscht wurden, und zeigt oben im Bereich die Gesamtanzahl an. Die Konsole kann über die Serververwaltungskonsole GroupShield-Eigenschaften und als unabhängiges Dienstprogramm auf einem Server, auf dem die Serververwaltungskonsole GroupShield-Eigenschaften nicht installiert ist, ausgeführt werden.

❑ **ANMERKUNG:** Die Schaltfläche Einstellungen ist nicht verfügbar, wenn die Konsole für das Scannen auf Anforderung aus der Serververwaltungskonsole GroupShield-Eigenschaften gestartet und nicht als unabhängiger Prozeß ausgeführt wird.

Über die Konsole können Sie einen Scanvorgang starten, beenden und anhalten. Sie können auch einen neuen Scanvorgang auf Anforderung auf einem anderen Microsoft Exchange-Server durchführen. Wenn der Scanvorgang von der Serververwaltungskonsole GroupShield-Eigenschaften gestartet wurde, wird er mit Hilfe der Registerkarte Auf Anforderung konfiguriert, und die Schaltfläche auf der Benutzeroberfläche der Konsole ist nicht verfügbar.

Die Oberfläche der Konsole für das Scannen auf Anforderung

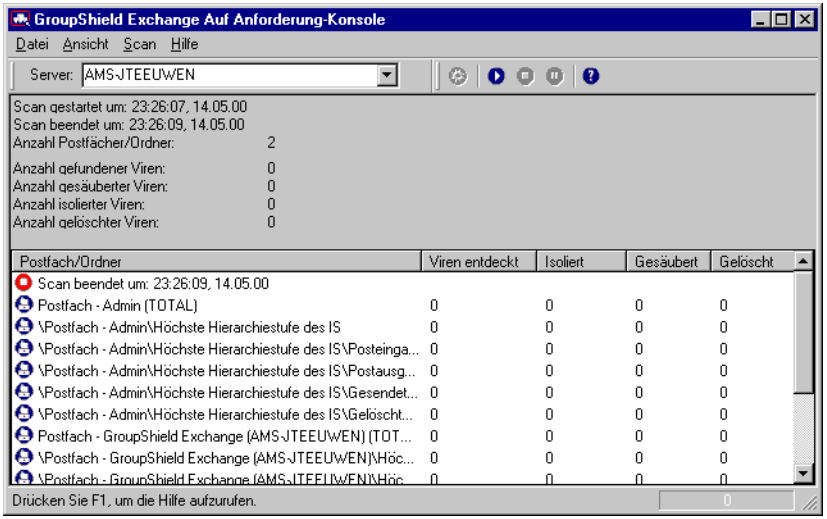

GroupShield Exchange Auf Anforderung-Konsole
Datei Ansicht Scan Hilfe
Server: AMS-JTEEUWEN
Scan gestartet um: 23:26:07, 14.05.00
Scan beendet um: 23:26:09, 14.05.00
Anzahl Postfächer/Ordner: 2
Anzahl gefundener Viren: 0
Anzahl gesäuberter Viren: 0
Anzahl isolierter Viren: 0
Anzahl gelöschter Viren: 0
Postfach/Ordner
Viren entdeckt
Isoliert
Gesäubert
Gelöscht
Scan beendet um: 23:26:09, 14.05.00
Postfach - Admin (TOTAL)
\Postfach - Admin\Höchste Hierarchiestufe des IS
\Postfach - Admin\Höchste Hierarchiestufe des IS\Posteinga...
\Postfach - Admin\Höchste Hierarchiestufe des IS\Postausg...
\Postfach - Admin\Höchste Hierarchiestufe des IS\Gesendet...
\Postfach - Admin\Höchste Hierarchiestufe des IS\Gelöscht...
Postfach - GroupShield Exchange (AMS-JTEEUWEN) (TOT...
\Postfach - GroupShield Exchange (AMS-JTEEUWEN)\Höc...
Drücken Sie F1, um die Hilfe aufzurufen.

Abbildung 4-12. GroupShield für Exchange-Konsole für das Scannen auf Anforderung

Die Konsole für das Scannen auf Anforderung gliedert sich in vier Hauptbereiche:

- Die Menüleiste ermöglicht es Ihnen, den GroupShield für Exchange-Server auszuwählen, der gescannt werden soll, die sichtbaren Symbolleisten der Konsole für das Scannen auf Anforderung festzulegen, einen Scanvorgang zu starten, abzubrechen und anzuhalten, sowie Hilfe zu erhalten. Eine vollständige Beschreibung der in den Menüs der Konsole verfügbaren Optionen finden Sie unter “Die Menüleiste“ auf Seite 92.
- Die Symbolleiste stellt dieselben Optionen wie die Menüleiste zur Verfügung. Eine vollständige Beschreibung der verfügbaren Optionen finden Sie unter “Die Symbolleiste“ auf Seite 93.
- Die Informationsanzeige zeigt einen zusammenfassenden Bericht, dem zu entnehmen ist, wie viele Viren auf dem Microsoft Exchange-Server gefunden, isoliert, gesäubert und entfernt wurden. Sie zeigt außerdem an, wann der Scanvorgang gestartet wurde und wann er endete, und wie viele Postfächer und öffentlichen Ordner dabei insgesamt durchsucht wurden.
- Das Ergebnisfenster. Eine vollständige Beschreibung der im Ergebnisfenster aufgezeichneten Daten finden Sie unter “Das Ergebnisfenster“ auf Seite 93.

Die Menüleiste

In den folgenden Abschnitten finden Sie eine Übersicht über die verschiedenen Menüoptionen, die über die Menüleiste verfügbar sind:

- Das Menü Datei auf Seite 92
- Das Menü Ansicht auf Seite 92
- Das Menü Scan auf Seite 92
- Das Menü Hilfe auf Seite 93

Das Menü „Datei“

- **Einstellungen** öffnet das Fenster Einstellungen, wenn die Konsole aus dem Programmverzeichnis GroupShield für Exchange heraus oder auf einem Remote-Server gestartet wird.

  Diese Option steht nicht zur Verfügung, wenn die Konsole über die Registerkarte Auf Anforderung in GroupShield-Eigenschaften gestartet wird.

- **Server wechseln** dient der Auswahl eines anderen Microsoft Exchange-Servers für den Scan.

  Unter “Wechseln des Zielservers“ auf Seite 98 erfahren Sie, wie Sie einen anderen Microsoft Exchange-Server für den Scan auswählen.

- **Beenden** schließt die Konsole für das Scannen auf Anforderung.

Das Menü „Ansicht“

- **Symbolleiste** blendet die Symbolleiste ein und aus.
- **Statusleiste** blendet die Statusleiste am unteren Ende des Fensters ein und aus.

Das Menü „Scan“

- **Start** startet den Scanvorgang
- **Anhalten/Fortsetzen** hält den Scanvorgang an. Wählen Sie denselben Befehl, um den Scanvorgang neu zu starten
- **Stop** beendet den Scanvorgang vorzeitig.

Das Menü „Hilfe“

- **Hilfethemen** öffnet die Hilfedatei der McAfee-Konsole für das Scannen auf Anforderung
- **Info** zeigt Urheberrechts- und Versionsinformationen zur Konsole für das Scannen auf Anforderung an.

Die Symbolleiste

Verwenden Sie das Kombinationsfeld Server, um den Microsoft Exchange-Server auszuwählen, den Sie scannen möchten.

öffnet das Fenster Einstellungen, wenn die Konsole aus dem Programmverzeichnis GroupShield für Exchange heraus oder auf einem Remote-Server gestartet wird.

Diese Schaltfläche steht nicht zur Verfügung, wenn die Konsole über die Serververwaltungskonsole GroupShield-Eigenschaften gestartet wird.

startet den Scanvorgang.

beendet den Scanvorgang vorzeitig.

hält den Scanvorgang an. Um einen angehaltenen Scanvorgang fortzusetzen, klicken Sie erneut auf .

öffnet das Dialogfeld Info.

Das Fenster zeigt Urheberrechtsdetails zur Konsole für das Scannen auf Anforderung sowie Systeminformationen über den aktuellen Server an und ermöglicht eine Verbindung mit der Network Associates-Website für technischen Support. Weitere Informationen erhalten Sie unter “Technischer Support“ auf Seite xix.

Klicken Sie im Dialogfeld Info auf **OK**, um zum Quarantine-Manager zurückzukehren.

Das Ergebnisfenster

Das Ergebnisfenster zeigt einen zusammenfassenden Bericht, dem zu entnehmen ist, wie viele Viren in jedem öffentlichen Ordner und in jedem Postfach auf dem Microsoft Exchange-Server gefunden, isoliert, gesäubert und entfernt worden sind.

Das Fenster gliedert sich in zwei klar getrennte Bereiche. Im oberen Teil des Fensters erhalten Sie einen zusammenfassenden Bericht über den Scanvorgang; der untere Fensterabschnitt enthält Ergebnisse für jeden einzelnen öffentlichen Ordner, der sich auf dem oben im Ergebnisfenster angegebenen Server befindet, und listet anschließend die Ergebnisse für jedes einzelne Postfach auf. Ebenso wird zu jedem Postfach, also Posteingang, Postausgang, gesendete und gelöschte Objekte, auch die Gesamtzahl der Viren aufgeführt.

Für jeden öffentlichen Ordner bzw. jedes Postfach erfolgt eine Aufschlüsselung der Zahlen nach gefundenen, isolierten, gesäuberten oder gelöschten Viren in Spalten auf der rechten Seite des Fensterausschnitts.

Die Spalte Postfach / Ordner enthält Angaben über Start- und Endzeit des Scanvorgangs. Außerdem kann sie Angaben über den Zeitpunkt einer vorzeitigen Beendigung des Scans sowie über Anhalte- und Neustartvorgänge enthalten.

Verwenden der Konsole für das Scannen auf Anforderung

Verwenden Sie die Konsole für das Scannen auf Anforderung von GroupShield für Exchange, um einen Scanvorgang auf Anforderung zu starten und seinen Verlauf zu überwachen.

❑ **ANMERKUNG:** McAfee empfiehlt, daß Sie für jeden Microsoft Exchange-Server, den Sie scannen möchten, auch Administratorrechte besitzen.

Um einen Scan auf Anforderung in der Konsole für das Scannen auf Anforderung von GroupShield-Eigenschaften zu starten, führen Sie folgende Schritte durch:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Auf Anforderung.

   Informationen über die Konfiguration eines Scanvorgangs mit neuen Einstellungen finden Sie unter den folgenden Themen:

- “Auswahl der zu scannenden Objekte“ auf Seite 72
- “Scanoptionen“ auf Seite 76
- “GroupShield für Exchange-Aktionen bei Viruserkennung“ auf Seite 79
- “Scannen neuer oder geänderter E-Mail-Anlagen“ auf Seite 81
- “Bericht auf Anforderung“ auf Seite 83.

ANMERKUNG: Um Änderungen zu speichern, die Sie an der Registerkarte Auf Anforderung vorgenommen haben, klicken Sie auf **Übernehmen**, bevor Sie die Konsole für das Scannen auf Anforderung öffnen.

2. Klicken Sie auf **Scankonsole** im unteren Teil des Fensters, um die Konsole zu starten.
3. Klicken Sie auf , um den Scanvorgang zu starten.

   Die Konsole teilt mit, wie viele Viren in jedem Informationsspeicher auf dem Microsoft Exchange-Server gefunden, isoliert, gesäubert und gelöscht wurden, und zeigt oben im Bereich die Gesamtsumme an. Weitere Informationen über die angezeigten Daten finden Sie unter "Das Ergebnisfenster" auf Seite 93.

ANMERKUNG: Sie können die Konsole für das Scannen auf Anforderung schließen und in GroupShield-Eigenschaften eine andere Registerkarte öffnen, während der Scanvorgang läuft. Der Scanner setzt seine Arbeit einfach im Hintergrund fort und meldet seine Ergebnisse an den GroupShield für Exchange Log Manager.

Verwenden der Konsole für das Scannen auf Anforderung aus dem Programmverzeichnis GroupShield für Exchange

Wird der Scanvorgang aus dem Programmverzeichnis Network Associates\GroupShield Exchange\i386 heraus gestartet, erfolgt die Konfiguration über das Fenster Einstellungen.

Mit dieser Methode können Sie einen Microsoft Exchange-Server scannen, auf dem GroupShield für Exchange nicht installiert ist.

Mit dem Fenster Einstellungen können Sie einen Scanvorgang für einen Server konfigurieren, auf dem GroupShield für Exchange nicht installiert ist. Die Schaltfläche Einstellungen der Auf Anforderung-Konsole ist nur dann verfügbar, wenn GroupShield für Exchange auf dem Server installiert ist und die Konsole aus dem Programmverzeichnis \i386 von GroupShield für Exchange heraus gestartet worden ist.

ANMERKUNG: McAfee empfiehlt, die Konsole für das Scannen auf Anforderung nur dann als unabhängigen Prozeß zu starten, wenn GroupShield für Exchange auf dem Zielserver nicht installiert ist.

Um die Konsole für das Scannen auf Anforderung aus dem GroupShield-Programmverzeichnis heraus zu starten, führen Sie diese Schritte aus:

1. Standardmäßig befindet sich die Konsole in dem folgenden Verzeichnis auf Ihrem Computer:

   ```
   C:\Programme\Network Associates\Tvd
   \GroupShield Exchange\i386\
   ```

2. Doppelklicken Sie zum Öffnen der Konsole im Verzeichnis \i386 von GroupShield für Exchange auf . Klicken Sie nach dem Starten der Konsole auf , um das Fenster Einstellungen zu öffnen, oder wählen Sie im Menü **Datei** den Befehl **Einstellungen**.

Um einen Scanvorgang mit Hilfe des Fensters Einstellungen zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Konsole für das Scannen auf Anforderung am folgenden Ort:

   ```
   C:\Programme\Network Associates\Tvd\GroupShield
   Exchange\i386
   ```

2. Klicken Sie auf , um das Fenster Einstellungen zu öffnen Abbildung 4-13 auf Seite 96).

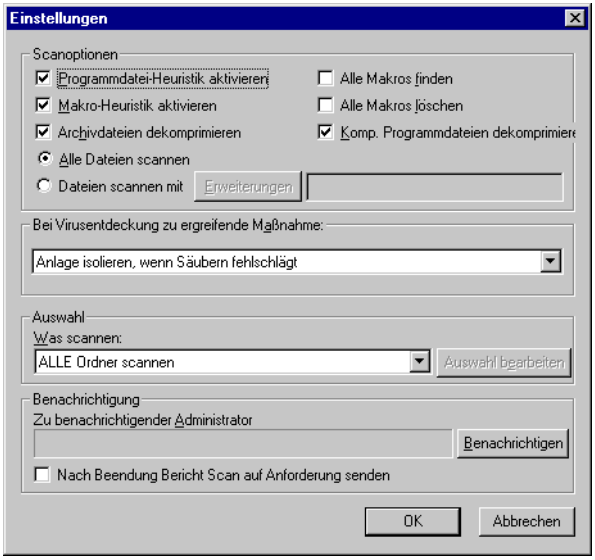


Abbildung 4-13. GroupShield für Exchange - Konsole für das Scannen auf Anforderung - Fenster Einstellungen

Das Fenster Einstellungen verfügt über die folgenden Optionen:

- Das Feld Scanoptionen teilt GroupShield für Exchange mit, welche Methoden der Virenerkennung während eines Scanvorgangs auf Anforderung eingesetzt werden sollen.

  Unter “Scanoptionen“ auf Seite 76 wird beschrieben, wie die Scanoptionen einzustellen sind.

- Das Kombinationsfeld Bei Viruserkennung zu ergreifende Maßnahme legt fest, welche Maßnahme GroupShield für Exchange als Reaktion auf ein während des Scanvorgangs auf Anforderung entdecktes Virus ergreifen soll.

  Unter “GroupShield für Exchange-Aktionen bei Viruserkennung“ auf Seite 79 finden Sie Informationen über die Maßnahmen, die GroupShield für Exchange ergreifen kann, wenn sie einen Scanvorgang auf Anforderung durchführt.

  ANMERKUNG: McAfee rät davon ab, die Option **Infektion protokollieren und ohne Säuberung fortfahren** zu verwenden.

- Das Kombinationsfeld Was scannen teilt GroupShield für Exchange mit, welche öffentlichen Ordner und Postfächer auf dem Zielserver durchsucht werden sollen.

  Unter “Auswahl der zu scannenden Objekte“ auf Seite 72 werden die Optionen des Kombinationsfeldes Was scannen näher beschrieben.

- Das Feld Benachrichtigungund zeigt den Namen eines Administrators an, der über eine Virusinfektion gegebenenfalls informiert werden soll.

  Wenn das Feld leer ist und Sie einen zu benachrichtigenden Administrator auswählen möchten, klicken Sie auf **Benachrichtigen**.

  ANMERKUNG: Unter Schritt 13 auf Seite 41 finden Sie weitere Informationen darüber, wie Sie angeben können, wer nach einem Scanvorgang auf Anforderung Benachrichtigungen erhalten soll.

- Aktivieren Sie das Kontrollkästchen **Nach Abschluß Bericht senden**, wenn GroupShield für Exchange an den im Feld Benachrichtigung gewählten Administrator einen Bericht senden soll, in dem die Ergebnisse des Scanvorgangs aufgeführt sind.

3. Klicken Sie auf **OK**, um die Einstellungen zu speichern und zur Konsole für das Scannen auf Anforderung zurückzukehren.

Ermitteln der Versionsinformationen

Um Versions- und Systeminformationen über das Dienstprogramm von GroupShield für Exchange Konsole für das Scannen auf Anforderung zu erhalten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Konsole für das Scannen auf Anforderung, und wählen Sie eine der folgenden Möglichkeiten:

- Klicken Sie in der Symbolleiste auf .
- Wählen Sie **Info** aus dem Menü **Hilfe**.

2. Im Dialogfeld Info haben Sie drei Möglichkeiten:

- Klicken Sie auf **Systeminfo**, um Informationen über den aktuell verwendeten Computer zu erhalten (beispielsweise die Größe des verfügbaren physischen Arbeitsspeichers.
- Klicken Sie auf **Technischer Support**, um eine Verbindung mit der Network Associates-Website herzustellen und technische Auskünfte über die Konsole für das Scannen auf Anforderung zu erhalten
- Studieren Sie die Versionsinformationen und klicken Sie auf **OK**, um zur Konsole für das Scannen auf Anforderung zurückzukehren.

Wechseln des Zielservers

Um einen anderen Microsoft Exchange-Server zum Scannen auszuwählen, führen Sie die folgenden Schritte aus:

1. Wählen Sie im Menü **Datei** den Befehl **Server wechseln**.
2. Suchen Sie im Dialogfeld Zielcomputer wählen nach dem Computer, den Sie scannen möchten, und wählen Sie ihn aus.

   Suchen Sie nach dem Computer mit derselben Methode, wie Sie dies in der Netzwerkumgebung von Microsoft Windows NT tun würden.
3. Klicken Sie auf **OK**, um die Serverauswahl zu übernehmen, und wählen Sie eine der folgenden Möglichkeiten:

- Klicken Sie auf , um das Fenster Einstellungen zu öffnen und den Scanvorgang zu konfigurieren
- Klicken Sie auf , um den Scanvorgang unter Verwendung der Standard- oder der zuletzt verwendeten Scaneinstellungen zu starten.

Durchführen eines Scanvorgangs auf Anforderung über die Befehlszeile

GroupShield für Exchange v4.5 ermöglicht die Festlegung eines Scanvorgangs auf Anforderung mit Hilfe der Befehlszeile. Mit dieser Scanmethode können Sie Scanvorgänge planen und die Software einen Scanvorgang durchführen lassen, sobald sich ein Administrator beim Server anmeldet.

❑ **ANMERKUNG:** Das vom Zeitplan zum Anmelden verwendete Konto muß ein Benutzerkonto und darf kein Systemkonto sein.

Um die Liste der Optionen an der Eingabeaufforderung anzuzeigen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Windows NT-Programmmenü, wählen Sie **MS-DOS-Eingabeaufforderung**, und wechseln Sie in das folgende Verzeichnis:

   <Laufwerk>:\Programme\Network Associates\Tvd\GroupShield Exchange\i386

   ❑ **ANMERKUNG:** Der aufgelistete Speicherort ist der Standardinstallationsort für GroupShield für Exchange. Wenn Sie die Software an einem anderen Ort installiert haben, wechseln Sie im Fenster Eingabeaufforderung zu diesem Verzeichnis.

   ---

2. Geben Sie dort den folgenden Befehl ein, um den ersten Teil der Liste mit Optionen anzuzeigen:

   ```
   odcmd /?
   ```

3. Um weitere Befehlszeilenoptionen anzuzeigen, geben Sie den folgenden Befehl ein:

   ```
   odcmd /? | more
   ```

Die folgende Tabelle beschreibt die an der Befehlszeile verfügbaren Optionen für das Scannen auf Anforderung. Für jede Option ist angegeben, wie und wo der Scanvorgang nach infizierten Dateien sucht. Verwenden Sie eine Kombination der Optionen, um den Scanvorgang Ihren Bedürfnissen anzupassen. Wenn der Eintrag in der Spalte **Standard** „Ein“ lautet, wird die Option automatisch ausgeführt und muß nicht zur Befehlszeile hinzugefügt werden. Sie können einige dieser Standardoptionen durch andere Optionen überschreiben.

Tabelle 4-1. Optionen für das Scannen auf Anforderung

Option	Beschreibung	Standard
/NOGUI	Diese Option bewirkt, daß der Fortschritt des Scanvorgangs nicht im Fenster Eingabeaufforderung angezeigt wird	Aus
/ADMIN	Diese Option legt den Benutzer fest, der Berichte über Virenerkennungen und das Scannen auf Anforderung erhält. Beispiel: /ADMIN=<Postfachname>. Wenn Sie einen Bericht über das Scannen auf Anforderung erhalten möchten, müssen Sie auch die Option /AUTOREPORT angeben	Aus
/EVENT	Diese Option legt den Namen des Ereignisses in der Liste geplanter Scanvorgänge fest. Beispiel: /EVENT=<Ereignisname>.	Aus
/TYPE	Diese Option legt den Typ des Scanvorgangs auf Anforderung fest, den GroupShield für Exchange durchführen soll. Wählen Sie eine der folgenden Optionen: **SCHEDULE** ist ein geplanter Scanvorgang auf Anforderung **MANUAL** ist ein sofortiger Scanvorgang auf Anforderung.	Die Option Manualist ist der Standardwert, wenn kein Typ ausgewählt wird
/DEFAULT	Diese Option verwendet standardmäßige GroupShield für Exchange-Scanvorgänge auf Anforderung. Bei der Standardoption werden maximale Sicherheitseinstellungen verwendet, was bedeutet, daß Scanvorgänge Systemressourcen zu Zeiten mit sehr hohem Nachrichtenverkehr stark belasten können.	Aus
/AUTOREPORT	Diese Option bewirkt, daß ein Bericht über ein Scannen auf Anforderung an den bei der Option /ADMIN angegebenen Benutzer gesendet wird	Aus

Tabelle 4-1. Optionen für das Scannen auf Anforderung

Option	Beschreibung	Standard
/OVF Aktion	Diese Option teilt GroupShield für Exchange mit, welche Aktion ausgeführt werden soll, wenn bei einem Scanvorgang auf Anforderung eine Virusinfektion festgestellt wird. Wählen Sie eine der folgenden Optionen: Mit **QM** wird die Nachricht isoliert. Mit **QA** wird die Anlage isoliert. Mit **CQM** wird versucht, die Nachricht zu säubern. Wenn die Nachricht nicht desinfiziert werden kann, wird die gesamte Nachricht isoliert. Mit **CQA** wird vesucht, die Anlage zu säubern. Wenn die Anlage nicht desinfiziert werden kann, wird sie an den Quarantäneort verschoben. Mit **DM** wird die Nachricht gelöscht. Mit **DA** wird die Anlage gelöscht. Mit **CDM** wird versucht, die Nachricht zu säubern. Wenn das mißlingt, wird sie gelöscht. Mit **CDA** wird versucht, die Anlage zu säubern. Wenn das mißlingt, wird sie gelöscht.	Die Option CQA ist der Standardwert, wenn keine /OVF-Aktion ausgewählt wird
/HEUR	Diese Option schaltet die Programmdatei-Heuristikoption ein, mit der GroupShield für Exchange heuristische Erkennungsmethoden verwendet, um potentielle neue Programmdateiviren zu erkennen.	Ein
/MACRO	Diese Option schaltet die Makro-Heuristikoption ein, mit der GroupShield für Exchange heuristische Erkennungsmethoden verwendet, um potentielle neue Makrodateiviren zu erkennen.	Ein

Tabelle 4-1. Optionen für das Scannen auf Anforderung

Option	Beschreibung	Standard
/ARC	Mit dieser Option wird innerhalb von Dateiarchiven (wie z.B. .ZIP oder .LZH-Dateien) gescannt. Wenn nur Dateien gescannt werden sollen, die bestimmte (Namens-)Erweiterungen haben, müssen Sie die erforderlichen Archivdateierweiterungen in die Liste der von der Software zu scannenden Dateierweiterungen aufnehmen.	Ein
/ZIPS	Mit dieser Option wird innerhalb komprimierter Dateien (z.B. Dateien, die mit PKLITE komprimiert wurden) gescannt. Wenn nur Dateien gescannt werden sollen, die bestimmte Erweiterungen haben, müssen Sie die erforderlichen Erweiterungen für komprimierte Dateien in die Liste der zu scannenden Dateierweiterungen aufnehmen.	Ein
/FAM	Mit dieser Option werden speziell Anlagen gescannt, die Makros enthalten, und diese werden als Viren behandelt, die nicht gesäubert werden können. Die Anlage wird isoliert und der Administrator über die Aktion benachrichtigt.	Aus
/DAM	Diese Option kann nur zusammen mit der Option Nach allen Makros suchen verwendet werden. Sie erkennt alle Makros und löscht sie, unabhängig davon, ob sie infiziert sind oder nicht.	Aus
/EXTN	Diese Option legt die Liste der Dateien fest, die GroupShield für Exchange scannen soll. Standardmäßig werden alle Dateien gescannt. Geben Sie die Erweiterungstypen in der Liste durch Kommas getrennt an. Beispiel: /EXTN=exe,dll,doc	Aus

Tabelle 4-1. Optionen für das Scannen auf Anforderung

Option	Beschreibung	Standard
/LIST	Diese Option legt die Liste der Microsoft Exchange-Nachrichtenspeicher fest, die GroupShield für Exchange scannen soll. Geben Sie die Speichernamen in der Liste durch Kommas getrennt an. Beispiel: /LIST=„\Öffentlicher Ordner1“,„Postfach1“ Namen öffentlicher Ordner müssen mit dem Zeichen „\“ beginnen und unterscheiden zwischen Groß- und Kleinschreibung. Namen, die Leerzeichen enthalten, müssen in Anführungszeichen gesetzt werden.	Standardmäßig werden alle Dateien gescannt
/PRIORITY	Diese Option legt die Priorität des Scanvorgangs fest. Wählen Sie eine der folgenden Prioritäten: **HIGH** **NORMAL** **LOW**	Wenn keine Priorität festgelegt ist, wird „Normal“ verwendet
/WHAT	Diese Option legt fest, wie GroupShield für Exchange die Liste der Objekte für die Option /LIST interpretieren soll. Wählen Sie eine der folgenden Optionen: Mit **SEL** werden nur aufgelistete Objekte gescannt Mit **EXPT** werden alle Objekte mit Ausnahme der aufgelisteten gescannt Mit **ALL** werden alle Objekte gescannt.	Wenn kein Objekt festgelegt ist, wird „ALL“ verwendet
/@ Antwortdatei	Diese Option gibt eine Antwortdatei an, aus der Befehle gelesen werden.	Aus

Beispiele für Befehlszeilen

Die folgenden Beispiele zeigen einige Möglichkeiten, wie Sie die Optionen zur Reaktion auf einen Virusangriff verwenden können.

Um einen Scanvorgang mit den auf der Registerkarte Auf Anforderung vorgenommenen Einstellungen auszuführen, führen Sie die folgenden Schritte aus:

1. Wechseln Sie an der Eingabeaufforderung in die GroupShield Exchange i386-Ebene.
2. Geben Sie den folgenden Befehl ein:

   ```
   odcmd /default
   ```

   ANMERKUNG: Um diesen Befehl verwenden zu können, muß GroupShield für Exchange bereits installiert sein.

Um einen Scanvorgang auf Anforderung auf einem Server auszuführen, auf dem GroupShield für Exchange nicht installiert ist, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei dem Server an, den GroupShield für Exchange scannen soll.
2. Verbinden Sie dann ein Netzlaufwerk mit einem GroupShield für Exchange-Server.
3. Wechseln Sie an der Eingabeaufforderung zum Installationsverzeichnis des GroupShield für Exchange-Servers, und geben Sie an der Befehlszeile den folgenden Befehl ein:

   ```
   odcmd /type=manual
   ```

   ANMERKUNG: Dieser Befehl führt einen Scanvorgang auf Anforderung unter Verwendung der maximalen Virenschutzeinstellungen von GroupShield für Exchange aus. McAfee empfiehlt, daß Sie diesen Befehl ausführen, wenn auf Ihren Microsoft Exchange-Server wenig Nachrichtenverkehr herrscht, um zu vermeiden, die Mailserver stark zu belasten.

Sie können die maximalen Sicherheitseinstellungen auf jedem Server überschreiben. GroupShield für Exchange muß nicht installiert sein. Im folgenden Beispielbefehl scannt GroupShield für Exchange einen Microsoft Exchange-Server, auf dem GroupShield für Exchange nicht installiert ist. Der Scanvorgang ist auf das Scannen von .ZIP-Dateien und die Verwendung heuristischer Technologie beschränkt, um Virusinfektionen in Programmdateien zu erkennen.

Führen Sie hierzu die folgenden Schritte durch:

1. Führen Sie Schritt 1 und Schritt 2 aus dem vorhergehenden Beispiel aus.
2. Geben Sie auf dem Zielserver an der Eingabeaufforderung die folgende Befehlszeile ein:

   ```
   odcmd /type=manual /heur /zips
   ```

Benachrichtigungen und Alarmmeldungen 5

GroupShield für Exchange kann Benutzer, die Sie angegeben haben, über die Aktion benachrichtigen, die die Software für eine infizierte Anlage unternommen hat. Es gibt zwei Arten der Benachrichtigung:

- Diejenigen, die während eines Scanvorgangs bei Zugriff gesendet werden.

  Sie können GroupShield für Exchange veranlassen, den Administrator zu benachrichtigen, wenn während eines Scanvorgangs bei Zugriff eine infizierte Datei isoliert wird. Der Administrator empfängt eine E-Mail-Nachricht mit folgendem Betrefftext:

  „WARNUNG - GroupShield-Ticket mit der Nummer OAx_xxxxxx_Servername wurde erstellt“

  Auch der Empfänger erhält die Originalnachricht, aber deren Anlage wird dabei durch die Ersatzanlage ALERT.TXT von GroupShield für Exchange ersetzt.

  ALERT.TXT enthält eine Ticket-Nummer, die mit derjenigen identisch ist, die in der E-Mail-Nachricht an den Administrator gesendet wurde. Der Empfänger sollte sich mit dieser Ticket-Nummer an den Administrator wenden, um den Speicherort der Anlage zu erfahren. Mit der Anlage kann dann so umgegangen werden, wie Sie das wünschen.

- Diejenigen, die während eines Scanvorgangs auf Anforderung gesendet werden.

  Wenn GroupShield für Exchange einen Scanvorgang auf Anforderung ausführt, können Sie über die folgenden Optionen festlegen, daß einer oder eine beliebige Kombination der angegebenen Benutzer per E-Mail benachrichtigt wird, wenn GroupShield für Exchange einen Virus entdeckt:

  – Autor – interner und externer
  – Empfänger – nur interner
  – Administrator (diejenigen, die auf der Registerkarte „Administration“ aufgelistet werden).

    Jede dieser Personen empfängt eine Benachrichtigung, die eine der nachfolgend aufgelisteten Betreffzeilen sowie entweder das Formular „avform“ von GroupShield für Exchange (sofern es installiert ist) oder eine Textnachricht enthält, die das Virus sowie die durchgeführte Aktion beschreibt.

Wurde die Anlage allerdings isoliert und nicht ohne weiterführende Maßnahme gelöscht oder protokolliert, so erhalten Autor und Empfänger die Originalnachricht, die jedoch statt der Originalanlage die Ersatzanlage ALERT.TXT von GroupShield für Exchange enthält.

Benachrichtigungen und GroupShield für Exchange-Aktionen

Der Betrefftext der Nachricht hängt von der Aktion ab, die GroupShield für Exchange unternommen hat. Über die Registerkarten Bei Zugriff und Auf Anforderung können Sie angeben, wie GroupShield für Exchange auf eine Virusinfektion reagieren soll, und über die Registerkarte Benachrichtigung können Sie den Betrefftext bearbeiten, der gesendet wird.

Eine Beschreibung der Benachrichtigungen, die je nach ergriffener Maßnahme nach dem Scanvorgang auf Anforderung von GroupShield für Exchange verschickt werden, finden Sie unter “Betreffzeilen”.

Betreffzeilen

Nur Administratoren werden während eines Scanvorgangs bei Zugriff von Virusinfektionen benachrichtigt. Sollen auch Absender und Empfänger darüber informiert werden, müssen Sie einen Scanvorgang auf Anforderung konfigurieren und initiieren. Die folgende Tabelle zeigt die Liste der auf der Registerkarte Benachrichtigung verfügbaren Betreffzeilen und die Aktionen der Registerkarten Bei Zugriff bzw. Auf Anforderung, denen diese Nachrichten entsprechen.

Tabelle 5-1. Betreffzeilen

Nachrichtenbetreff	Bei Zugriff-Aktion	Auf Anforderung-Aktion
Anlage kann nicht gesäubert werden	Anlage isolieren, wenn Desinfizierung fehlschlug	Anlage isolieren, wenn Desinfizierung fehlschlug
Anlage gesäubert *	Anlage isolieren, wenn Desinfizierung fehlschlug	Anlage isolieren, wenn Desinfizierung fehlschlug
Anlage isoliert	Anlage isolieren, ohne Desinfizierung zu versuchen	Anlage isolieren, ohne Desinfizierung zu versuchen

Tabelle 5-1. Betreffzeilen

Nachrichtenbetreff	Bei Zugriff-Aktion	Auf Anforderung-Aktion
Nachricht isoliert	Nicht zutreffend **	Nachricht isolieren, ohne Desinfizierung zu versuchen
Nachricht/Anlage wurde gelöscht	Anlage löschen, wenn Desinfizierung fehlschlug Infizierte Anlage löschen	Anlage löschen, wenn Desinfizierung fehlschlug Nachricht löschen, wenn Säuberung fehlschlug Infizierte Anlage löschen Infizierte Nachricht löschen
Virus gefunden, aber nichts unternommen	Infektion protokollieren und ohne Säuberung fortfahren	Infektion protokollieren und ohne Säuberung fortfahren

* Die Anlage wurde nicht isoliert, da sie gesäubert wurde. Der Betreff der Meldung informiert den Administrator darüber, daß die Anlage ein Virus enthielt, GroupShield für Exchange die Anlage aber erfolgreich gesäubert und dann an den vorgesehenen Empfänger gesendet hat.

** Bei einem Scan bei Zugriff werden nur E-Mail-Anlagen überprüft.

Führen Sie folgende Schritte aus, um die Warnmeldungen zu konfigurieren, die GroupShield für Exchange sendet, sobald ein Virus entdeckt wurde:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Benachrichtigung (Abbildung 5-1 auf Seite 110).

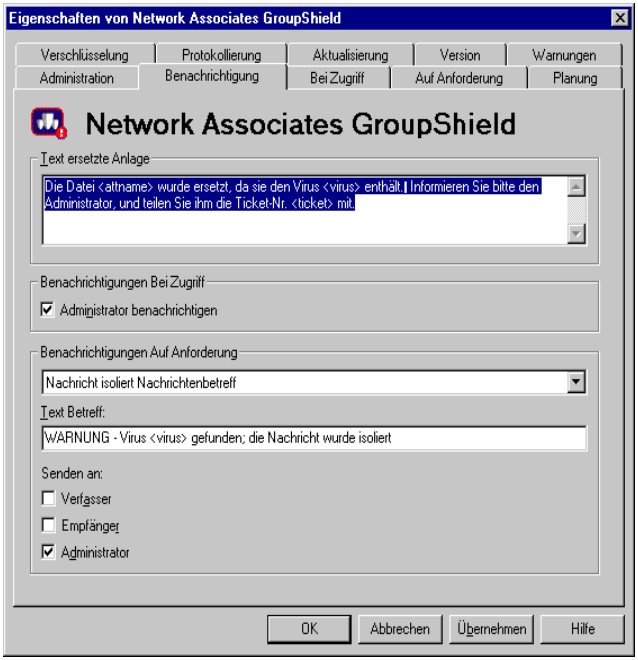


Abbildung 5-1. GroupShield-Eigenschaften - Registerkarte Benachrichtigung

2. Zur Bearbeitung der Ersatzanlage wählen Sie einen der Texte aus, die GroupShield für Exchange zum Einfügen anbietet. Eine Liste der verfügbaren Texte finden Sie unter “Einfügbare Ersatztexte für Benachrichtigungen“ auf Seite 112.

3. Deaktivieren Sie das Kontrollkästchen **Administrator benachrichtigen**, damit GroupShield für Exchange nicht weiterhin während eines Scanvorgangs bei Zugriff Benachrichtigungen an die Administratoren sendet, die auf der Registerkarte Administration aufgelistet sind.

4. Führen Sie folgende Teilschritte im Feld Benachrichtigungen auf Anforderung aus, um die einzelnen Betreffzeilen zu bearbeiten, die GroupShield für Exchange bei Durchführung einer Scanoperation auf Anforderung sendet:

    a. Wählen Sie im Kombinationsfeld einen Nachrichtenbetrefftext aus.

    b. Verwenden Sie die einfügbaren Ersatztexte von GroupShield für Exchange, um den Betrefftext zu bearbeiten.

c. Aktivieren oder deaktivieren Sie die Benutzer, die diese Nachricht erhalten sollen. Wählen Sie aus folgenden Optionen:

– **Autor**

– **Empfänger**

– **Administrator**

d. Wiederholen Sie die Schritte a) bis c) für jede Benachrichtigung, die Sie ändern möchten.

5. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll. Klicken Sie auf eine andere Registerkarte.

Führen Sie folgende Schritte aus, wenn Sie die Standardbenachrichtigungen ändern möchten:

1. Wählen Sie im Kombinationsfeld einen Nachrichtenbetrefftext aus.
2. Verwenden Sie die einfügbaren Ersatztexte von GroupShield für Exchange, um den Betrefftext zu bearbeiten.
3. Aktivieren oder deaktivieren Sie die Kontrollkästchen vor den Benutzern, die diese Nachricht erhalten sollen. Wählen Sie eine der folgenden Optionen:

- **Autor**
- **Empfänger**
- **Administrator**

4. Wiederholen Sie die Schritte 1 bis 3 für jede Benachrichtigung, die Sie ändern möchten.
5. Verwenden Sie die einfügbaren Ersatztexte von GroupShield für Exchange, um den Betrefftext zu bearbeiten.

ANMERKUNG: Jede aus einer E-Mail-Nachricht entfernte Anlage wird durch die Nachricht ALERT.TXT ersetzt.

Einfügbare Ersatztexte für Benachrichtigungen

Verwenden Sie eine Kombination der folgenden Einfügungen, um eine Benachrichtigung mit einer ALERT.TXT-Anlage zu modifizieren.

Text	Beschreibung
<Virus>	Der Name des gefundenen Virus
<attfile>	Der Name der Anlage, z. B. C:\DATEINAME\XX.BAT
<attname>	Der Dateiname der Anlage, z. B. XX.BAT
<from>	Der Name des Absenders *
<to>	Die Liste der Empfänger *
<subject>	Der Text des Nachrichtenbetreffs *
<time>	Die Uhrzeit der Nachricht *
<messagestore>	Der Name des Postfachs, z. B. Helga Schmidt *
<folder>	Der Name eines Öffentlichen Ordners *
<qtine>	Der Name des Quarantäneorts
<datenow>	Das Datum der Benachrichtigung
<timenow>	Die Uhrzeit der Benachrichtigung
<ticket>	Die von der Warnung erstellt Ticket-Nummer

Objekte, die mit einem Sternchen "*" gekennzeichnet sind, stehen nur für Benachrichtigungen zur Verfügung, die von einem Auf Anforderung-Scanvorgang erstellt wurden.

Serveradministration und Protokollierung 6

Administration (Registerkarte)

Die Registerkarte Administration wird automatisch angezeigt, wenn Sie die Serververwaltungskonsole GroupShield-Eigenschaften starten. Die Seite ist in drei Felder unterteilt:

- **Postfach des Administrators** - dient dazu, Postfächer, die Benachrichtigungen über von Viren infizierte Nachrichten / Anlagen sowie die Ergebnisse eines Scanvorgangs auf Anforderung empfangen, zu der Liste der Postfächer des Administrators hinzuzufügen oder aus dieser Liste zu entfernen.
- **Quarantäneort** - dient dazu, das Quarantäneverzeichnis von GroupShield für Exchange bzw. den Speicherort der Quarantänedatenbank von GroupShield für Exchange zu wechseln, wo alle blockierten E-Mail-Nachrichten oder infizierten Anlagen abgelegt werden, für die weitere Aktionen vorgesehen sind.
- **Schutz vor Dienstverweigerung** - gibt an, wie lange (in Minuten) der GroupShield für Exchange-Dienst versuchen soll, eine E-Mail-Anlage zu scannen, bevor er die Anlage an den Quarantäneort sendet. Maßnahmen zur Verhinderung von Dienstverweigerungen finden Sie unter “Verhindern einer Dienstverweigerung (des Scan-Dienstes)“ auf Seite 118.

Auswählen von Administratorpostfächern für den Empfang von Benachrichtigungen

Um festzulegen, welche Administratorpostfächer bei eine Virusattacke benachrichtigt werden und einen Scanbericht auf Anforderung erhalten sollen, führen Sie folgende Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften. Die Registerkarte Administration wird als Standardseite (Abbildung 6-1 auf Seite114) angezeigt.

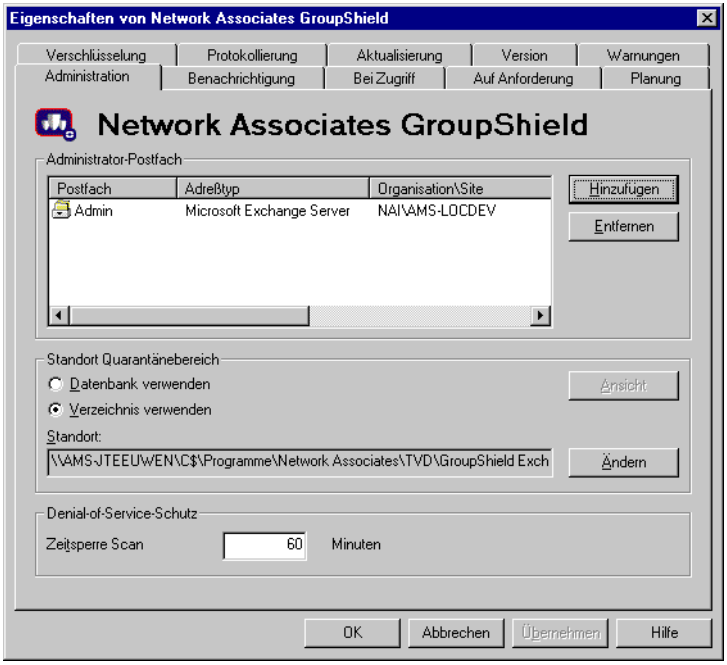


Abbildung 6-1. GroupShield-Eigenschaften - Registerkarte „Administration“

2. Klicken Sie im Feld Postfach des Administrators auf **Hinzufügen**, um das Dialogfeld Benachrichtigung auswählen (Abbildung 6-2) anzuzeigen.

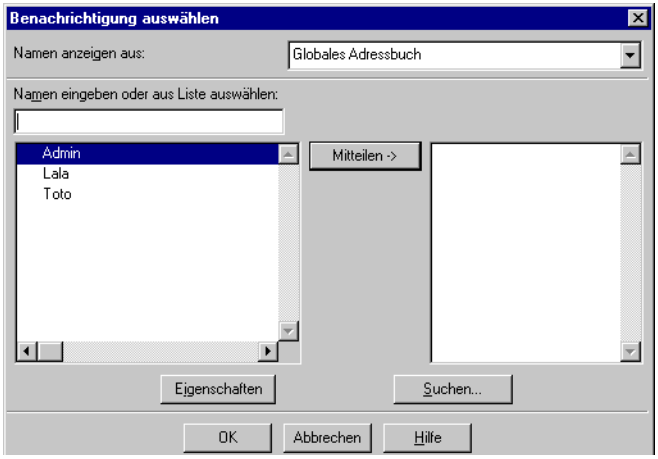


Abbildung 6-2. Registerkarte „Administration“ - Dialogfeld „Benachrichtigung auswählen“

3. Wählen Sie die E-Mail-Verteilerliste aus, in der Sie Postfächer auswählen möchten.
4. Jetzt können Sie GroupShield für Exchange auf zwei Arten mitteilen, an welche Postfächer Benachrichtigungen gesendet werden sollen:

- Geben Sie den Postfachnamen in das entsprechende Textfeld ein. Trennen Sie je zwei Namen durch ein Semikolon (;)
- Markieren Sie den Postfachnamen im Adreßbuch. Klicken Sie auf **Suchen**, um die Postfächer zu finden, die Sie hinzufügen möchten.

5. Klicken Sie auf **Benachrichtigen>>->**, um den Postfachnamen im rechten Listenfeld anzuzeigen.
6. Wiederholen Sie die Schritte 4 und 5 so oft, wie nötig.
7. Klicken Sie auf **OK**, um zur Registerkarte Administration zurückzukehren.
8. Wenn Sie auf der Registerkarte Administration alle gewünschten Einstellungen vorgenommen haben, führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und das Eigenschaftenfenster von GroupShield schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und das Eigenschaftenfenster von GroupShield schließen möchten.
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen übernehmen möchten, ohne das Eigenschaftenfenster von GroupShield zu schließen. Nehmen Sie weitere Einstellungen auf der Registerkarte Administration vor, oder klicken Sie auf eine andere Registerkarte.

Ergänzende Informationen

- Wenn Sie möchten, daß GroupShield für Exchange keine Benachrichtigungen mehr an ein Postfach sendet, markieren Sie den Postfachnamen und klicken auf **Entfernen**. Es muß immer mindestens ein Postfach aufgelistet werden.
- Sie können GroupShield für Exchange dazu veranlassen, blockierte Nachrichten und infizierte Anlagen an einen sicheren Quarantäneort im System zu senden. Dabei haben Sie die Wahl, isolierte Objekte an die Quarantine Manager-Datenbank, auf die über die Registerkarte Administration zugegriffen werden kann, oder an ein Quarantäneverzeichnis senden zu lassen.

Auswählen einer Isolierungsmethode und eines Quarantäneortes

Um anzugeben, auf welche Weise und an welchem Ort GroupShield für Exchange eine infizierte E-Mail-Nachricht oder -Anlage ablegen soll, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften. Standardmäßig wird die Registerkarte Administration angezeigt.
2. Aktivieren Sie im Feld Quarantäneort eines der folgenden Optionsfelder:

- **Datenbank verwenden**

  Klicken Sie auf **Ansicht**, um McAfee Quarantine Manager (Abbildung 6-3) zu öffnen.

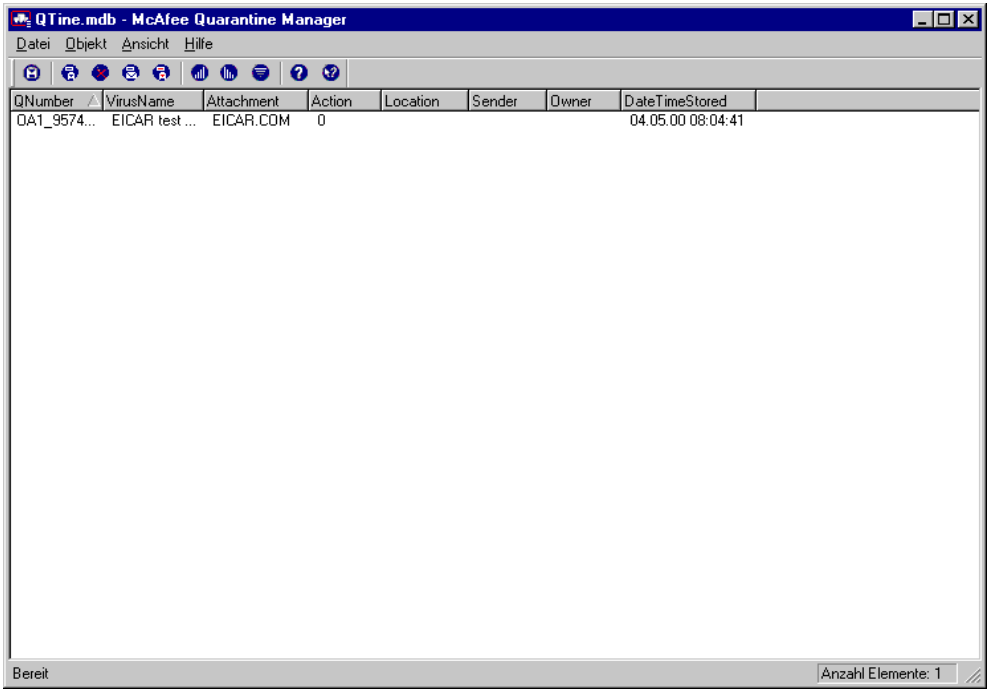

QTine.mdb - McAfee Quarantine Manager
Datei Objekt Ansicht Hilfe
QNumber VirusName Attachment Action Location Sender Owner DateTimeStored
OA1_9574... EICAR test ... EICAR.COM 0 04.05.00 08:04:41
Bereit
Anzahl Elemente: 1

Abbildung 6-3. McAfee Quarantine Manager

- **Verzeichnis verwenden**

3. Führen Sie folgende Teilschritte aus, wenn Sie den Quarantäneort Ihres Systems ändern möchten:

- Wenn die Option **Datenbank verwenden aktiviert** ist, klicken Sie auf **Ändern**.

  a. Es wird das Dialogfeld Datenbank suchen (Abbildung 6-4 auf Seite117) angezeigt. Wechseln Sie zum gewünschten Speicherort, und klicken Sie auf **Öffnen**.

Abbildung 6-4. Registerkarte „Administration“ - Dialogfeld „Datenbank suchen“

  b. Klicken Sie auf **OK**, um zur Registerkarte Administration zurückzukehren.

- Wenn die Option **Verzeichnis verwenden** aktiviert ist, klicken Sie auf **Ändern**.

  a. Es wird das Dialogfeld Nach Ordner suchen (Abbildung 6-5) angezeigt. Verwenden Sie die Explorer-Ansicht, um nach dem gewünschten Speicherort zu suchen.

  –

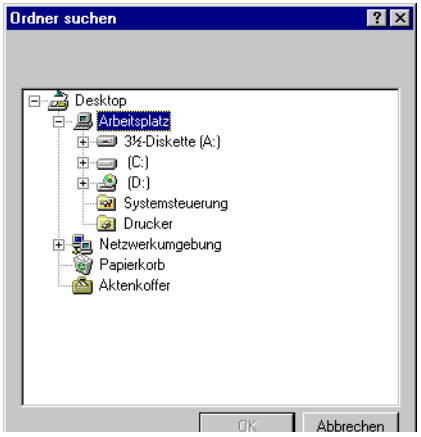


Abbildung 6-5. Registerkarte „Administration“ - Dialogfeld „Nach Ordner suchen“

b. Klicken Sie auf **OK**, um zur Registerkarte Administration zurückzukehren.

4. Wenn Sie auf der Registerkarte Administration alle gewünschten Einstellungen vorgenommen haben, führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und das Eigenschaftenfenster von GroupShield schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und das Eigenschaftenfenster von GroupShield schließen möchten.
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen übernehmen möchten, ohne das Eigenschaftenfenster von GroupShield zu schließen. Sie können dann eine andere Registerkarte wählen.

Ergänzende Informationen

- Um die Quarantänefunktion zu deaktivieren, aktivieren Sie eine der beiden folgenden Optionen auf den Registerkarten Bei Zugriff und Auf Anforderung:
  - **Anlage löschen, wenn Desinfizierung fehlschlug**
  - **Infizierte Anlage löschen**

ANMERKUNG: McAfee empfiehlt, die Option Infektion protokollieren und weiter ohne Säuberung weder auf der Registerkarte Bei Zugriff noch auf der Registerkarte Auf Anforderung zu aktivieren.

- Sie können GroupShield für Exchange anweisen, Benachrichtigungen zu senden, wenn ein Objekt während eines Scanvorgangs auf Anforderung isoliert wurde.
- Falls auf demselben Server auch ein McAfee Desktop-Virenschutzprogramm (beispielsweise NetShield für Windows NT) installiert ist, empfiehlt McAfee, das Verzeichnis **qtinewrk** von den Scanvorgängen des Desktop-Scanners auszuschließen. Andernfalls entdeckt die NetShield-Software die infizierten Objekte, die in das GroupShield für Exchange-Quarantäneverzeichnis verschoben wurden. In Ihrer Dokumentation wird beschrieben, wie Verzeichnisse von Scanvorgängen ausgeschlossen werden.

Verhindern einer Dienstverweigerung (des Scan-Dienstes)

Eine Anlage, für deren Scannen übermäßig viel Zeit benötigt wird, kann zu einer teilweisen Dienstverweigerung des Virenschutzprogramms führen. Eine Dienstverweigerung verhindert, daß die Virenschutz-Scan-Engine irgendeine andere Anlage scannt, die sich in der Warteschlange befindet. E-Mail-Nachrichten, die keine Anlagen haben, können während des Scanvorgangs gelesen werden.

Führen Sie folgende Schritte aus, um eine Dienstverweigerungsattacke zu verhindern:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften. Die Registerkarte Administration wird als Standardseite (Abbildung 6-2 auf Seite114) angezeigt.

2. Geben Sie in das Feld Schutz vor Dienstverweigerung die maximale Zeit in Minuten ein, die die Scanengine mit dem Scannen einer Anlage verbringen darf.

   Sie können als maximale Anzahl Minuten den Wert 2880 eingeben (dies entspricht 2 Tagen). Alle Anlagen, bei deren Scannen diese Zeit überschritten wird, werden automatisch isoliert. Die Virenschutz-Scanengine setzt ihre Aktivitäten dann jeweils mit neuen Anlagen fort. Damit sichergestellt ist, daß die Ergebnisse im McAfee Log Manager protokolliert werden, sollten Sie den Network Associates Log Service (Protokollierdienst) neustarten. Informationen über den Neustart von Diensten finden Sie unter “Beenden und Neustart der Dienste“ auf Seite 48.

3. Wenn Sie auf der Registerkarte Administration alle gewünschten Einstellungen vorgenommen haben, führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und das Eigenschaftenfenster von GroupShield schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und das Eigenschaftenfenster von GroupShield schließen möchten.
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen übernehmen möchten, ohne das Eigenschaftenfenster von GroupShield zu schließen.

Behandlung verschlüsselter E-Mail-Nachrichten

Über die Registerkarte Verschlüsselung können Sie bestimmen, wie GroupShield für Exchange mit verschlüsselten E-Mail-Nachrichten umgehen soll. Beispielsweise kann die Software angewiesen werden, alle verschlüsselten E-Mail-Nachrichten zu isolieren oder ausgewählten Postfächern zu erlauben, diese verschlüsselte E-Mail-Nachrichten ungescannt zu senden.

Um festzulegen, wie GroupShield für Exchange mit verschlüsselten E-Mail-Nachrichten verfahren soll, führen Sie folgende Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Verschlüsselung, um die Registerkarte Verschlüsselung anzuzeigen (Abbildung 6-6 auf Seite120).

Abbildung 6-6. GroupShield-Eigenschaften - Registerkarte „Verschlüsselung“

2. Verwenden Sie im Feld Auf Anforderung-Vertrauen das Kombinationsfeld Vertrauen, um GroupShield für Exchange anzugeben, wie mit verschlüsselten E-Mail-Nachrichten umgegangen werden soll. Wählen Sie eine der folgenden Optionen:

- **Jeder vertrauen** ignoriert von allen Postfächern gesendeten verschlüsselte Nachrichten.

  McAfee empfiehlt Ihnen, diese Option nicht zu aktivieren. GroupShield für Exchange kann keine verschlüsselten Anlagen scannen.

- **Aufgelisteten Postfächern** vertrauen ignoriert nur verschlüsselte Nachrichten, die von den aufgelisteten Postfächern gesendet wurden. Führen Sie folgende Schritte aus, um Postfächer hinzuzufügen, denen vertraut wird:

a. Wählen Sie im Kombinationsfeld Vertrauendie Option **Aufgelisteten Postfächern vertrauen** aus.

b. Klicken Sie auf **Postfach hinzufügen**, um das Dialogfeld Treuhänder auswählenanzuzeigen (Abbildung 6-7 auf Seite121).

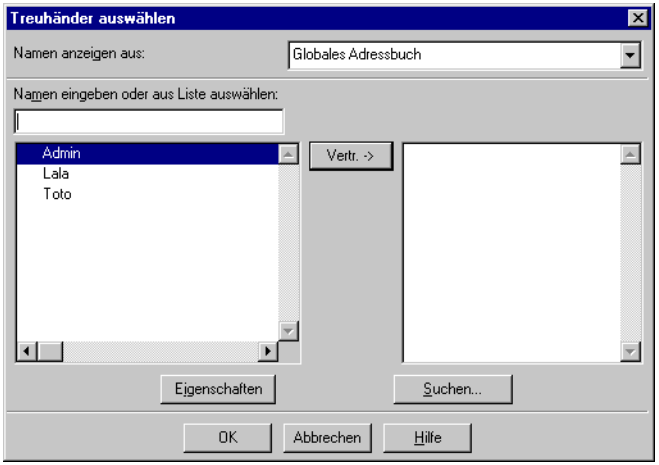


Abbildung 6-7. Registerkarte „Verschlüsselung“ - Dialogfeld „Treuhänder auswählen“

c. WählenSiedieE-Mail-Verteilerlisteaus,inderSiePostfächerauswählen möchten.

d. AnschließendkönnenSieGroupShieldfürExchangeaufzweiArtenmitteilen, welchenPostfächerndasVersendenverschlüsselterE-Mail-Nachrichten gestattet werden soll:

– GebenSiedenPostfachnamenindasentsprechendeTextfeldein.TrennenSie je zwei Namen durch ein Semikolon (;)

– Markieren Sie den Postfachnamen im Adreßbuch. Klicken Sie auf **Suchen**, um die Postfächer zu finden, die Sie hinzufügen möchten.

e. Klicken Sie auf **Vertrauen>>**, damit der Postfachname im rechten Listenfeld angezeigt wird.

f. Wiederholen Sie die Schritte b) bis e) je nach Bedarf.

g. Klicken Sie auf **OK**, um zur Registerkarte Verschlüsselung zurückzukehren.

- **Keiner vertrauen** isoliert jede von irgendeinem Postfach gesendete verschlüsselte Nachricht.

3. Aktivieren Sie im Feld Vertrauen bei Zugriff die Option **Jeder mit Network Associates PGP™ verschlüsselten E-Mail vertrauen**, damit bei einem Scanvorgang bei Zugriff GroupShield für Exchange allen E-Mail-Nachrichten vertraut, die mit der Network Associates PGP-Verschlüsselungssoftware verschlüsselt wurden.

   Das mit öffentlichen Schlüsseln arbeitende PGP-Kryptografiesystem der Software ermöglicht es, Nachrichten sicher zu übertragen und vor unbefugtem Lesen zu schützen. Digitale Signaturen, die zu Nachrichten hinzugefügt werden, garantieren deren Echtheit und Datenintegrität. PGP-E-Mail-Plug-Ins unterstützen die Mehrzahl der gängigen E-Mail-Anwendungen, sodass Benutzer und Empfänger nicht gezwungen sind, ihre E-Mail-Programme zu wechseln.

4. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll. Klicken Sie auf eine andere Registerkarte.

Ergänzende Informationen

- Wenn GroupShield für Exchange E-Mail-Nachrichten scannen soll, die von einem Postfach gesendet wurden, dem bisher vertraut wurde, wählen Sie dieses Postfach in der Spalte Postfach aus und klicken dann auf **Postfach entfernen**.

Ermitteln der GroupShield Exchange-Versionsinformationen

Die Registerkarte Version zeigt Versionsinformationen über die GroupShield für Exchange-Serversoftware und das Scanmodul an.

Um die Registerkarte Version zu öffnen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Version, um die Registerkarte Version anzuzeigen (Abbildung 6-8 auf Seite 123).

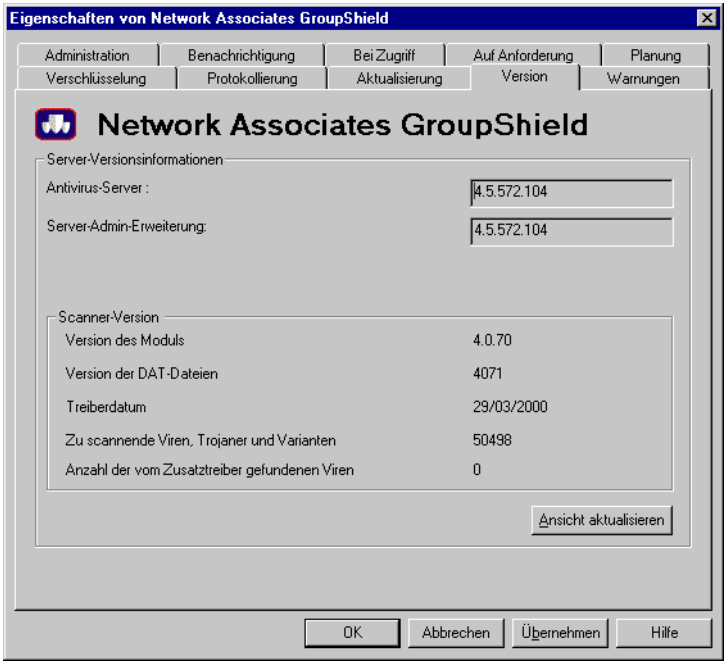


Abbildung 6-8. GroupShield-Eigenschaften - Registerkarte „Version“

Die angezeigten Informationen enthalten:

Über den Server:

- **Antivirus-Server** ist die Version der Virenschutzsoftware von GroupShield für Exchange, die auf den Clients dieses Servers installiert ist.
- **Servererweiterungen Administration** ist die Version der Serververwaltungssoftware von GroupShield für Exchange.
- **Antivirus-Benutzeradministrationserweiterung** ist die Version der Benutzerverwaltungssoftware von GroupShield für Exchange.

Die Antivirus-Benutzeradministrationserweiterung wird nur angezeigt, wenn Sie dies während des Upgrades von GroupShield für Exchange v4.0.4 auf GroupShield für Exchange v4.5 festlegen.

Über die Scan-Engine:

- Modulversion ist die Version der Engine im Virenschutzscanner.
- **Dat-Version** ist die Version der Virusinformationsdatei.
- **Treiberdatum** ist das Datum der letzten Treiberaktualisierung.
- **Zu scannende Viren, Trojanische Pferde und Varianten** bezeichnet die Anzahl der Viren sowie sonstigen bösartigen Codes, die von GroupShield für Exchange erkannt werden.
- **Nein. „Viren, die durch zusätzlichen Treiber gefunden wurden“** bezeichnet die Anzahl der durch zusätzliche Treiber gefundenen Viren.

2. Wenn Sie alle gewünschten Informationen gesehen haben, führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie während dieser Arbeitssitzung auf anderen Seiten vorgenommen haben, und das Eigenschaftenfenster von GroupShield zu schließen.
- Klicken Sie auf **Abbrechen**, wenn Sie die auf anderen Seiten vorgenommenen Änderungen verwerfen und das Eigenschaftenfenster von GroupShield schließen möchten.
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen übernehmen möchten, die Sie vor dem Öffnen der Registerkarte Version auf anderen Seiten vorgenommen haben, ohne das Eigenschaftenfenster von GroupShield von GroupShield zu schließen. Sie können dann auf eine andere Registerkarte klicken.

Protokollieren von Virenschutz- und Systemereignissen

Die GroupShield für Exchange verwendet McAfee Log Manager, um das Ereignisprotokoll von GroupShield für Exchange auszuwerten. Ereignisse werden unter folgenden Bedingungen protokolliert:

- Wenn die GroupShield für Exchange-Dienste gestartet oder beendet werden
- Wenn die McAfee-Virusdefinitionsdateien (.DAT-Dateien) aktualisiert werden
- Wenn in der Serververwaltungskonsole GroupShield-Eigenschaften Änderungen an den Einstellungen von GroupShield für Exchange vorgenommen werden
- Wenn das System ausfällt
- Wenn ein Auf Anforderung-Scanvorgang gestartet oder beendet wird
- Wenn ein zeitlich geplanter Auf Anforderung-Scanvorgang ausgeführt wird

Wenn GroupShield für Exchange während eines Scanvorgangs auf Anforderung oder auf Zugriff eine Virusinfektion entdeckt, werden die folgenden Informationen protokolliert:

- Der Name des Microsoft Exchange-Informationsspeichers (Information Store), in dem der Virus entdeckt wurde
- Der Name des Virus
- Die Aktion, die GroupShield für Exchange unternommen hat.

ANMERKUNG: Verwenden Sie die Registerkarten Bei Zugriff und Auf Anforderung der GroupShield-Eigenschaften, um GroupShield für Exchange mitzuteilen, welche Aktion sie unternehmen soll, wenn sie eine Virus entdeckt hat.

Weitere Informationen über McAfee Log Manager, dessen Funktionen und ihre Verwendung finden Sie unter “Arbeiten mit Log Manager“ auf Seite 194. Das Verfahren zur Konfigurierung der Log Manager-Ausgabe ist im Abschnitt “Konfigurieren der McAfee Log Manager-Ausgabe” weiter unten beschrieben.

Konfigurieren der McAfee Log Manager-Ausgabe

Geben Sie mit Hilfe der Registerkarte Protokollierung der GroupShield-Eigenschaften an, welche Ereignisse und Virenschutzaktivitäten von McAfee Log Manager protokolliert werden sollen. Sie haben folgende Möglichkeiten:

- Anpassen des Ergebnisses im Log Manager im Feld Grad.
- Dem Log Manager angeben, für welche GroupShield für Exchange-Komponenten er Ereignisse protokollieren soll.
- Festlegen eines Speicherorts auf dem Server für die Log Manager-Datenbank.
- Festlegen des Limits (maximale Anzahl der Einträge oder Tage), bei dessen Überschreiten eine Kopie der ältesten Einträge erstellt und das Protokoll aktualisiert wird.

Um die vom Log Manager aufgezeichneten Ereignisse zu konfigurieren und die Aufzeichnungen anzuzeigen, führen Sie folgende Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Protokollierung, um die Registerkarte Protokollierung anzuzeigen (Abbildung 6-9 auf Seite126).

Abbildung 6-9. GroupShield-Eigenschaften - Registerkarte „Protokollierung“

2. Aktivieren Sie im Feld Optionen für die Ereignisprotokollierung eine oder mehrere der folgenden Optionen, um die Ausgabe anzupassen, die im Log Manager im Feld Gradangezeigt wird:

- Systemfehler
- Fehler
- Warnungen
- Information

3. Aktivieren Sie im Feld Protokollierungsoptionen Komponenten eine oder mehrere der folgenden Optionen, um den Log Manager anzuweisen, welche Komponenten von GroupShield für Exchange er protokollieren soll:

- **Antivirus-Server** - zeichnet jedes Ereignis auf, das während eines Scanvorgangs bei Zugriff oder auf Anforderung innerhalb des Network Associates GroupShield für Exchange-Dienstes stattfindet, sowie jedes Ereignis, das während einer Aktualisierung einer Virusdefinitionsdatei (.DAT-Datei) innerhalb des Network Associates GroupShield Online-Aktualisierungs-Dienstes stattfindet.

- **Serveradministration** - repräsentiert Änderungen, die innerhalb der Serverwaltungskonsole GroupShield-Eigenschaften vorgenommen wurden.

ANMERKUNG: Klicken Sie auf **Im NT-Ereignisprotokoll aufzeichnen**, wenn alle von der Option Antivirus protokollierten Ereignisse im Microsoft Windows NT-Ereignisprotokoll aufgezeichnet werden. Um das Windows NT-Ereignisprotokoll anzuzeigen, öffnen Sie das **Startmenü** und zeigen auf **Programme**. Dann wählen Sie im Menü **Verwaltung** den Befehl **Ereignisanzeige**.

---

4. Wählen Sie im Feld Protokollkonfiguration eine der folgenden Optionen aus, und geben Sie dann den Wert ein, ab dem GroupShield für Exchange die ältesten Einträge des Protokolls überschreiben soll.

- **Maximale Einträge**
- **Maximale Tage**

5. Klicken Sie auf **Protokoll anzeigen**, um den Log Manager (Abbildung 6-10) zu öffnen. Weitere Informationen über den Log Manager und die Möglichkeiten, sich Ergebnisse benutzerdefiniert anzeigen zu lassen, finden Sie unter “Arbeiten mit Log Manager“ auf Seite 194.

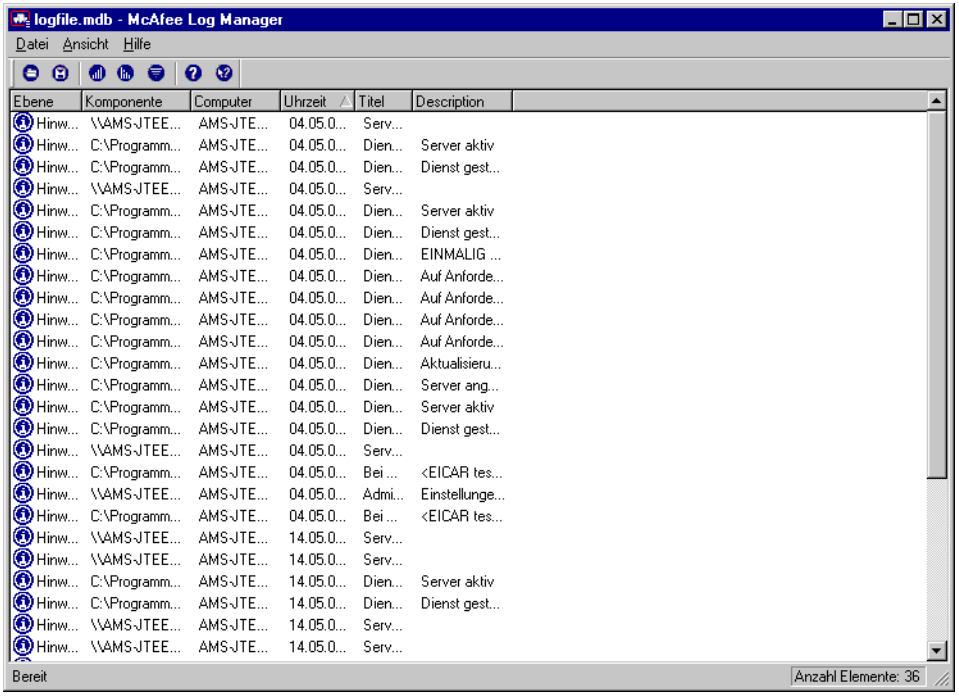


Abbildung 6-10. McAfee Log Manager

6. Um McAfee Log Manager-Daten an eine andere Stelle auf dem Server zu verschieben, klicken Sie auf ..., und verwenden dann das Dialogfeld Datenbank suchen (Abbildung 6-11), um an die Stelle im Dateisystem zu wechseln, wo die Protokolldatei abgelegt werden soll.

Abbildung 6-11. Registerkarte „Protokollierung“ - Dialogfeld „Datenbank suchen“

ANMERKUNG: Um den Speicherort der Utility-Datenbank des Log Manager zu ändern und der Software die Protokollierung von Virusbenachrichtigungen bei Zugriff und auf Anforderung in der neuen Log Manager-Datenbank zu ermöglichen, müssen Sie den GroupShield für Exchange-Dienst neu starten. Entsprechende Anleitungen finden Sie in Kapitel 2, „Erste Schritte“.

7. Markieren Sie schließlich den Namen der Datenbank, so daß er im Feld Dateiname erscheint, und klicken Sie dann auf **Öffnen**.

8. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll. Sie können dann eine andere Registerkarte zur Bearbeitung wählen.

Automatische Aktualisierung der .DAT-Dateien 7

Um den bestmöglichen Schutz vor Viren zu gewährleisten, hält McAfee die .DAT-Dateien mit den Virusdefinitionen, welche GroupShield für Exchange zur Virenerkennung verwendet, ständig auf dem neuesten Stand. Obwohl die hier beschriebene Software über eine Technologie verfügt, die in der Lage ist, auch bisher unbekannte Arten von Viren oder bösartigen Code aufzuspüren, tauchen immer wieder neue Arten von Viren und anderer Agentensoftware auf. Häufig kann die vorhandene Software diese Viren nicht erkennen, da die mitgelieferten Dateien mit den Virusdefinitionen (.DAT-Dateien) nicht mehr auf dem aktuellen Stand sind. Um einen maximalen Schutz zu gewährleisten, empfiehlt McAfee nachdrücklich, diese Dateien regelmäßig zu updaten.

❑ **ANMERKUNG:** Der Ausdruck „Update“ bezeichnet die Integration neuer Versionen der .DAT-Dateien in Ihre Software, während „Upgrade“ sich auf den Übergang zu neuen Produktversionen bezieht, also auf ausführbare Programmdateien und Daten. McAfee bietet Ihnen während der gesamten Nutzungsdauer Ihres Produkts einen kostenlosen Updateservice für die .DAT-Dateien. Das schließt garantiert allerdings nicht, daß die .DAT-Dateien immer kompatibel mit älteren Produktversionen sind. Durch beständiges Upgrade der Software auf die neueste Produktversion und Update der .DAT-Dateien sorgen Sie für umfassenden Schutz während der Dauer Ihres Softwareabonnements oder Wartungsplans.

Die Registerkarte Aktualisierung gibt GroupShield für Exchange zum einen die Methode an, nach der die Virusdefinitionsdateien (.DAT-Dateien) aktualisiert werden sollen, und gibt zum anderen an, welche GroupShield für Exchange-Server aktualisiert werden sollen.

Das Aktualisieren der .DAT-Dateien erfolgt in zwei Phasen: In der ersten Phase geben Sie GroupShield für Exchange an, welche Server aktualisiert werden sollen. In der zweiten Phase konfigurieren Sie die Aktualisierungsmethode.

Inkrementelle Aktualisierungen

GroupShield Exchange v4.5 verwendet die neue AutoUpdate-Technologie, um die aktualisierten .DAT-Dateien auf intelligente Weise zu installieren. Anstatt die gesamten Dateien zu ersetzen, ergänzt die Software die .DAT-Dateien um diejenigen Teile, die sich noch nicht auf Ihrem Computer befinden. Inkrementelle Aktualisierungen entlasten Ihren Exchange-Server, da sie zu einem geringeren Übertragungsvolumen führen.

Weitere Informationen über die neue AutoUpdate-Technologie finden Sie unter “McAfee-Aktualisierungsdienstprogramme“ auf Seite 263.

Hinzufügen von GroupShield für Exchange-Servern, um .DAT-Dateien zu aktualisieren

Mit GroupShield für Exchange lassen sich die .DAT-Dateien auf mehreren Microsoft Exchange-Servern gleichzeitig aktualisieren. Vergewissern Sie sich, daß mindestens die folgenden Voraussetzungen in bezug auf den Zielserver erfüllt werden:

- Sie verfügen über Administratorrechte, d. h. Lese / Schreibberechtigungen für den Zielserver.
- Der Dienst Online-Update von GroupShield für Exchange wird ausgeführt.

ANMERKUNG: Einem GroupShield für Exchange 4.0.4-Server ist es nicht möglich, die McAfee-Virusdefinitionen (.DAT-Dateien) eines GroupShield für Exchange-Servers der Version 4.5 zu aktualisieren. Der Versuch einer solchen Aktualisierung schlägt fehl und alle mit dem Aktualisierungs-Assistenten vorgenommenen Einstellungen gehen verloren.

Führen Sie folgende Schritte aus, um einen GroupShield für Exchange-Server hinzuzufügen, der seine Virusdefinitionsdateien aktualisieren soll:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte **Aktualisierung**, um die Registerkarte **Aktualisierung** anzuzeigen (Abbildung 7-1).

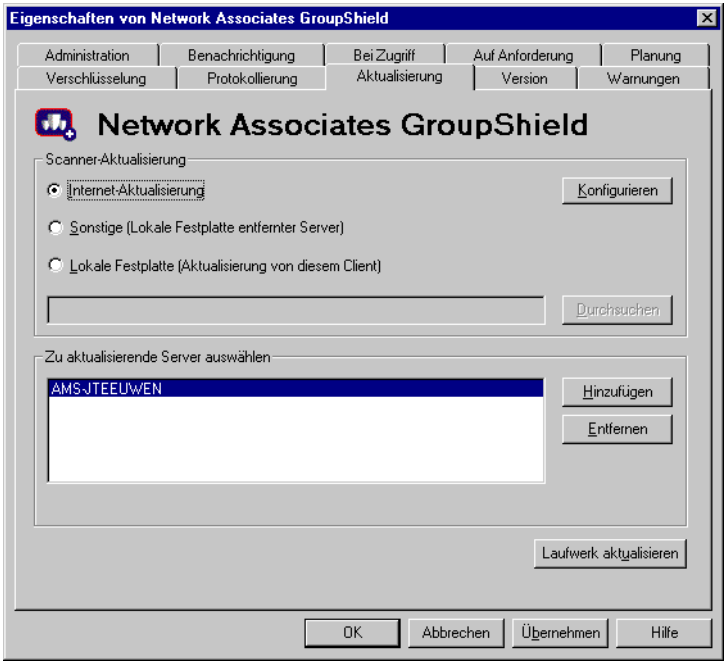


Abbildung 7-1. GroupShield-Eigenschaften - Registerkarte „Aktualisierung“

2. Klicken Sie im Feld Zu aktualisierende Server auswählen auf **Hinzufügen**.
3. Geben Sie im Dialogfeld Computer auswählen (Abbildung 7-2) den Namen eines Computers ein, oder wählen Sie einen Namen in der angezeigten Liste aus.

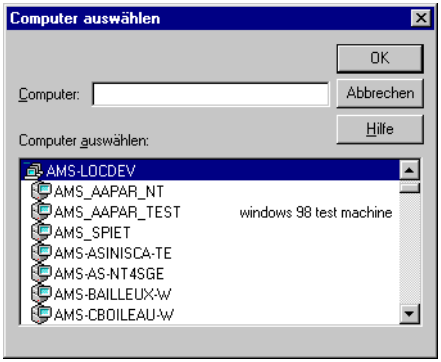


Abbildung 7-2. Registerkarte „Aktualisierung“ - Dialogfeld „Computer auswählen“

4. Klicken Sie auf **OK**.
5. Wiederholen Sie die Schritte 2 bis 4 so oft, wie nötig.

   Um einen Server zu entfernen, markieren Sie ihn in der Serverliste auf der Registerkarte Aktualisierung und klicken dann auf **Entfernen**.

Auswählen einer Aktualisierungsmethode

Die AutoUpdate-Technologie stellt mehrere Verfahren zur Aktualisierung der .DAT-Dateien zur Verfügung. Zur Auswahl einer der Methoden führen Sie die folgenden Schritte aus:

1. Markieren Sie mindestens einen Server für die Aktualisierung.
2. Geben Sie im Feld Scanner-Aktualisierung den Speicherort der aktualisierten Virusinformationsdateien (.DAT-Dateien) an. Führen Sie einen der folgenden Schritte aus:

- **Internet-Aktualisierung** bezieht die neuen Virusinformationsdateien über das Internet von der Network Associates-Website.

  Die zugehörige Anleitung finden Sie unter “Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) über das Internet“ auf Seite 133.

- **Sonstige (Lokale Festplatte entfernter Server)** aktualisiert die Virusinformationsdateien vom Microsoft Exchange-Server aus.

  Die zugehörige Anleitung finden Sie unter “Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) von einem entfernten Server aus“ auf Seite 134.

- **Lokale Festplatte (Aktualisierung von diesem Client)** aktualisiert die Virusinformationsdateien vom lokalen Computer aus.

  Die zugehörige Anleitung finden Sie unter “Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) vom lokalen Computer aus“ auf Seite 138.

❑ **ANMERKUNG:** Sie müssen sicherstellen, daß die aktualisierten Virusdefinitionsdateien (.DAT-Dateien) bereits dekomprimiert sind, bevor Sie versuchen, sie auf einem anderen Computer zu installieren.

Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) über das Internet

Die Option Internet-Aktualisierung überträgt die aktualisierten Virusinformationsdateien über das Internet von der Network Associates-Website.

Ändern Sie die Einstellungen für die Aktualisierungsquelle und den Proxyserver und konfigurieren Sie zeitlich geplante Aktualisierungen der .DAT-Dateien aus dem Internet.

Um die Virusdefinitionsdateien (.DAT-Dateien) über die Network Associates-Website zu aktualisieren, gehen Sie wie folgt vor:

1. Aktivieren Sie im Feld Scanner-Aktualisierung das Optionsfeld **Internet-Aktualisierung**.
2. Klicken Sie auf **Konfigurieren**.

   Der Aktualisierungs-Assistent wird mit dem Bildschirm Internet-Einstellungen gestartet (Abbildung 7-3 auf Seite 133).

   Mit Hilfe des Assistenten können Sie die Einstellungen für die Aktualisierungsquelle und den Proxyserver ändern sowie zeitlich geplante Aktualisierungen der .DAT-Dateien aus dem Internet konfigurieren.

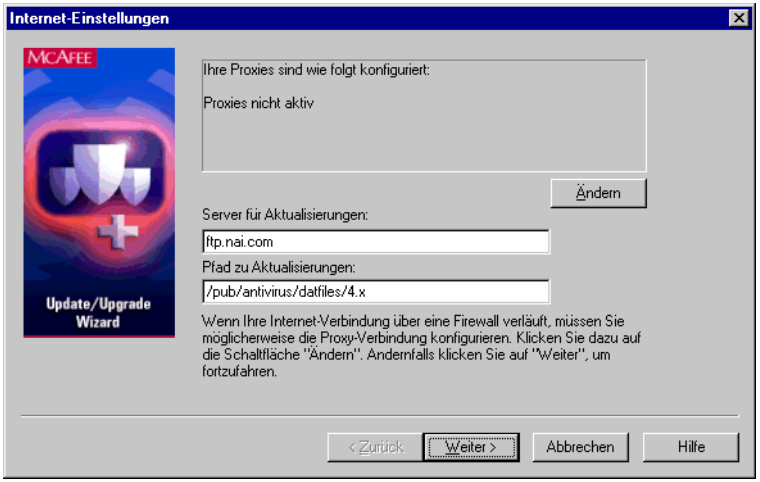


Abbildung 7-3. Aktualisierungs-Assistent - Seite „Internet-Einstellungen“

3. Wenn Sie die Verbindung zum Internet über einen Firewall herstellen, müssen Sie möglicherweise die Proxyserververbindung konfigurieren. Klicken Sie dazu in der Seite Internet-Einstellungen auf **Ändern**.

4. Aktivieren Sie im Dialogfeld Proxy-Information ändern (Abbildung 7-4) das Kontrollkästchen **Mittels Proxyserver verbinden**.

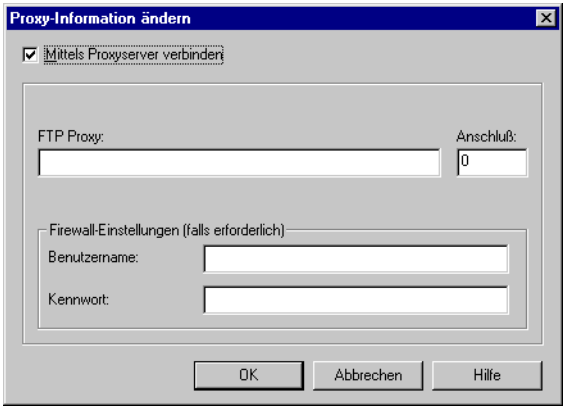


Abbildung 7-4. Seite „Internet-Einstellungen“ - Dialogfeld „Proxy-Information ändern“

5. Geben Sie den Namen und den Anschluß für den FTP-Proxy ein, und geben Sie den Benutzernamen und das Kennwort ein, bevor Sie eine Verbindung zum Internet herstellen.

WICHTIG: Geben Sie bei der Angabe des Aktualisierungsquellverzeichnisses keinen Laufwerksbuchstaben ein. Alle Netzwerkpfade müssen in der UNC-Schreibweise angegeben werden.

Klicken Sie auf **OK**, um zur Seite Internet-Einstellungen zurückzukehren.

6. Klicken Sie auf **Weiter>**, um die Seite Konfiguration geplanter Aktualisierung (Abbildung 7-7) anzuzeigen, und fahren Sie dann mit Schritt 1 auf Seite 136 fort.

Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) von einem entfernten Server aus

1. Aktivieren Sie im Feld Scanner-Aktualisierung die Option **Sonstige (Lokale Festplatte entfernter Server)**.

2. Wählen Sie in der Serverliste einen oder mehrere Server zum Aktualisieren aus.

3. Klicken Sie auf **Konfigurieren**, um die Seite Aktualisierung konfigurieren (Abbildung 7-5) anzuzeigen.

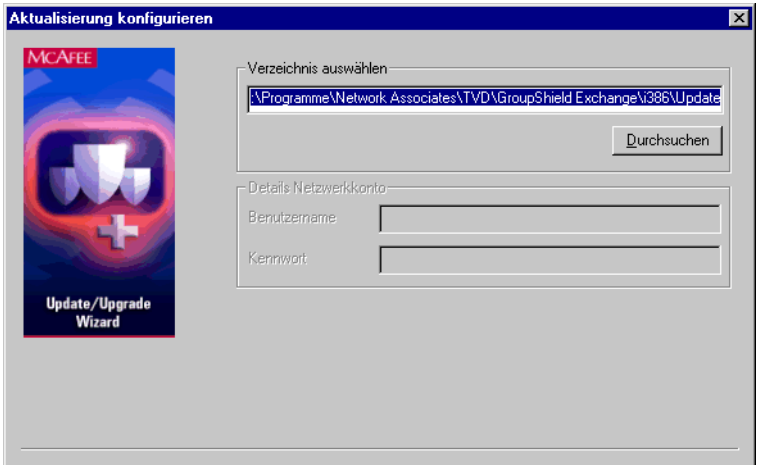


Abbildung 7-5. Aktualisierungs-Assistent - Seite „Aktualisierung konfigurieren“

4. Führen Sie einen der folgenden Schritte aus:

- Legen Sie das Verzeichnis fest, in dem GroupShield für Exchange die Aktualisierungsdateien empfangen soll. Wechseln Sie auf der Seite Aktualisierung konfigurieren über **Durchsuchen** zu dem Verzeichnis, in dem GroupShield für Exchange die Aktualisierungsdateien vorfinden soll, oder geben Sie den Pfad direkt in das Textfeld **V**erzeichnis auswählen ein.

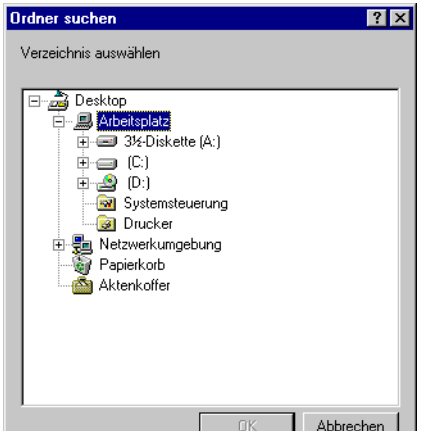


Abbildung 7-6. Seite „Aktualisierung konfigurieren“ - Dialogfeld „Nach Ordner suchen“

Geben Sie bei Bedarf den Benutzernamen und das Kennwort ein, mit denen auf das Aktualisierungsverzeichnis zugegriffen wird. Für Windows-Netzwerkdomänen können Sie einen Domänennamen gefolgt von einem Benutzernamen eingeben, wie z.B. DOMAENE\benutzername. Geben Sie bei der Angabe des Aktualisierungsquellverzeichnisses keinen Laufwerksbuchstaben ein. Alle Netzwerkpfade müssen in der UNC-Schreibweise angegeben werden.

- Klicken Sie auf **Weiter>**, um die Seite Konfiguration geplanter Aktualisierung (Abbildung 7-7 auf Seite 136) anzuzeigen, und fahren Sie dann mit Schritt 1 in "Zeitliche Planung der Aktualisierungen" fort.

Zeitliche Planung der Aktualisierungen

Der Bildschirm Konfiguration geplanter Aktualisierung ist unabhängig davon, ob Sie die Datei über das Internet oder einen Remote-Server aktualisieren, Teil des Aktualisierungs-Assistenten. Sobald Sie festgelegt haben, auf welche Weise GroupShield für Exchange die McAfee-Virusdefinitionsdateien (.DAT-Dateien) aktualisieren soll, können Sie unter Verwendung der Seite Konfiguration geplanter Aktualisierung der Software den Zeitpunkt mitteilen, zu dem die Aktualisierung erfolgen soll.

Um den gewünschten Zeitpunkt für die Aktualisierung einer .DAT-Datei anzugeben, führen Sie die folgenden Schritte aus:

1. Aktivieren Sie in der Seite Konfiguration geplanter Aktualisierung (Abbildung 7-7 auf Seite 136) entsprechend Ihren Anforderungen eine Kombination der folgenden Optionen:

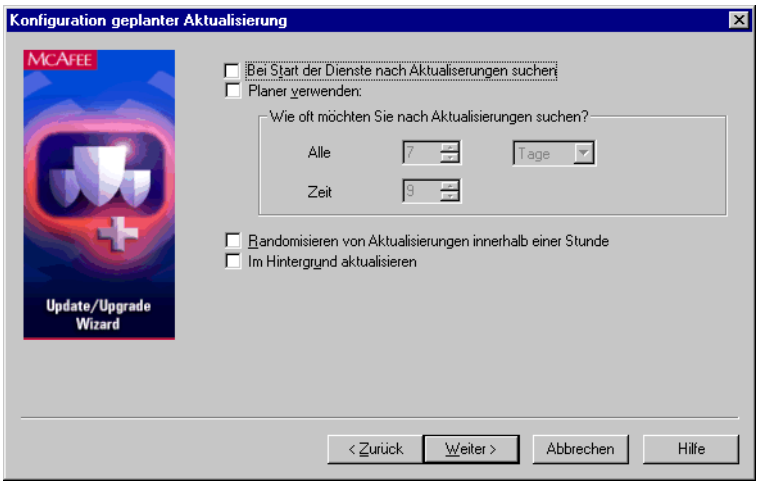


Abbildung 7-7. Aktualisierungs-Assistent - Seite „Konfiguration geplanter Aktualisierung"

- **Beim Systemstart auf Aktualisierungen prüfen** weist die Software an, bei jedem Start des Network Associates GroupShield Online-Aktualisierungs-Dienstes nach aktualisierten .DAT-Dateien zu suchen.
- **Zeitplaner verwenden** bewirkt, daß die .DAT-Dateien in von Ihnen vorgegebenen Intervallen aktualisiert werden.

  Geben Sie die Anzahl Tage oder Stunden ein, die zwischen zwei Aktualisierungen liegen sollen, oder verwenden Sie die Pfeilsymbole, um den gewünschten Wert auszuwählen.

  ANMERKUNG: McAfee empfiehlt, die .DAT-Dateien mindestens einmal pro Woche zu aktualisieren, um einen maximalen Schutz gegen Virenattacken zu gewährleisten.

- **Zufälliger Beginn der Aktualisierungen innerhalb einer Stunde** verhindert, daß Clientcomputer versuchen, die Aktualisierung zum selben Zeitpunkt zu beginnen. Diese Option bedeutet, daß die Clientaktualisierung so eingestellt ist, daß sie zufällig innerhalb einer Zeitspanne bis zu einer Stunde ab dem Zeitpunkt beginnt, den Sie in der Option **Zeitplaner verwenden** festgelegt haben.

  GroupShield für Exchange versucht, innerhalb dieser Stunde die Aktualisierung durchzuführen, sofern der Server zum gewählten Zeitpunkt nicht bereits eine solche Operation durchführt. Wenn zum Zeitpunkt dieses Versuchs Scanvorgänge ablaufen, wartet die Software und startet anschließend einen erneuten Versuch. Dies wird solange wiederholt, bis der Versuch zum Erfolg führt.
- **Hintergrundaktualisierung** aktualisiert die .DAT-Dateien, ohne daß während einer zeitlich geplanten Aktualisierung eine Benachrichtigung erfolgt.

2. Klicken Sie auf **Weiter>**.

   Der Bildschirm Upgrade-Auswahl zeigt die Aktualisierungskonfiguration an, die Sie gerade festgelegt haben.
3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **<Zurück**, wenn Sie eine getätigte Einstellung ändern möchten.
- Klicken Sie auf **Fertigstellen**, wenn Sie die Konfiguration bestätigen und auf dem ausgewählten Server speichern und zur Registerkarte Aktualisierung zurückkehren möchten. Wenn Sie mehrere Server ausgewählt haben, wird die Konfiguration auf jedem dieser Server dupliziert.

4. Führen Sie einen der folgenden Schritte aus:

- **Klicken Sie auf Treiber aktualisieren**, um die Aktualisierung zu starten.

  ANMERKUNG: Wenn Sie GroupShield für Exchange auf einem Computer installiert haben, auf dem zuvor die Version v4.0.4 von GroupShield für Exchange installiert war, ist das Kontrollkästchen **Clients aktualisieren** auf der Registerkarte **Aktualisierung** verfügbar. Weitere Informationen über das Aktualisieren von Clients finden Sie im Benutzerhandbuch, das zusammen mit Ihrer Kopie der Version v4.0.4 der Software ausgeliefert wird.

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll. Klicken Sie auf eine andere Registerkarte.

Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) vom lokalen Computer aus

Aktualisieren Sie die Virusdefinitionsdateien (.DAT-Dateien) von einem lokalen Computer aus, wenn Sie zu einem früheren Stand der .DAT-Dateien zurückkehren oder dekomprimierte .DAT-Dateien installieren möchten, die durch ein anderes McAfee-Virenschutzprogramm aus dem Internet heruntergeladen worden sind.

Um einen lokalen Computer zur Aktualisierung von Virusdefinitionsdateien (.DAT-Dateien) zu verwenden, führen Sie folgende Schritte aus:

1. Wählen Sie auf der Registerkarte Aktualisierung die Option **Lokale Festplatte (Aktualisierung von diesem Client)**.
2. Geben Sie einen Verzeichnispfad in das Textfeld ein, oder klicken Sie auf **Durchsuchen**, um zum gewünschten Verzeichnis zu wechseln, von aus dem Sie die aktualisieren Virusdefinitionsdateien übertragen möchten.
3. Wählen Sie die Microsoft Exchange-Server aus, die Sie aktualisieren möchten.

Falls sich ein zu aktualisierender Server nicht in der Liste findet, klicken Sie auf **Hinzufügen**, und folgen Sie den Anweisungen unter "Hinzufügen von GroupShield für Exchange-Servern, um .DAT-Dateien zu aktualisieren".

4. Klicken Sie auf **Treiber aktualisieren**, um die Aktualisierungen an den oder die ausgewählten Server zu senden.

5. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, wenn Sie die Änderungen speichern und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Abbrechen**, wenn Sie die Änderungen verwerfen und die Serververwaltungskonsole GroupShield-Eigenschaften schließen möchten
- Klicken Sie auf **Übernehmen**, wenn Sie die Änderungen speichern möchten und die Serververwaltungskonsole GroupShield-Eigenschaften geöffnet bleiben soll. Klicken Sie auf eine andere Registerkarte.

Viruswarnsystem 8

Mehrere Informationsmethoden

Die McAfee-Virenschutzsoftware bietet mehrere Methoden, um Sie über die Fortschritte und die Ergebnisse von Scanaktivitäten zu informieren. Beispiel:

- Sie können sich die Ergebnisse eines Scanvorgangs nach dessen Beendigung ansehen, indem Sie McAfee Log Manager öffnen.
- Sie können sich die Scanergebnisse ansehen, so wie sie auftreten, indem Sie im Systemmonitor von GroupShield für Exchange die Statistiken bei Zugriff und auf Anforderung anzeigen. Allerdings werden Sie bei keiner dieser Methoden sofort gewarnt, wenn der Scanner ein Virus entdeckt hat.
- Sie können über die Konsole für ein Scannen auf Anforderung bei GroupShield für Exchange eine Echtzeitanzeige des Verlaufs eines Scanvorgangs auf Anforderung beobachten.

Sofern Sie nicht eine Datei oder einen Ordner scannen, die oder der Sie besonders interessiert, ist es unwahrscheinlich, daß Sie sehr viel Zeit damit verbringen möchten, den Bildschirm auf Anzeichen einer Infektion zu beobachten. Darüber hinaus gibt es kein Gegenstück, mit dem der Verlauf von Scanvorgängen bei Zugriff beobachtet werden kann.

Es ist Aufgabe von Warnungs-Manager, Sie direkt zu benachrichtigen, daß der Scanner einen Virus entdeckt hat oder daß der Zeitplan auf ein Problem gestoßen ist. Warnungs-Manager ist ein eigenständiges Modul, das in GroupShield für Exchange integriert und für die Verwendung auf Servern vorgesehen ist, die unter Windows NT, Version v4.0, oder Windows 2000 laufen.

Überblick über die Warnmethoden

Warnungs-Manager bietet Ihnen eine Auswahl unterschiedlicher Methoden, mit denen der Scanner Benachrichtigungen senden kann, sobald er ein Virus entdeckt hat. Dazu gehören:

- **Weiterleiten**. Diese Methode ermöglicht es Ihnen, Meldungen zur weiteren Verteilung direkt an einen anderen Computer derselben Domäne zu senden, auf dem Warnungs-Manager ausgeführt wird. Diese Methode bietet sich an, wenn Sie einen bestimmten Computer oder eine bestimmte MIS-Abteilung (MIS = Management-Informationssystem) als Ausgangspunkt für die Alarmmeldungen festlegen möchten, die von der Virenschutzsoftware erstellt werden.

- **Netzwerkmeldung**. Mit dieser Methode können Sie eine Alarmmeldung als Broadcast-Meldung über das gesamte Netzwerk senden. Diese Methode ist standardmäßig aktiviert. Der Computer, auf dem Warnungs-Manager installiert ist, empfängt die Benachrichtigung, nachdem der Scanner ein Virus entdeckt hat.
- **E-Mail**. Diese Methode ermöglicht es Ihnen, eine Alarmmeldung an bestimmte E-Mail-Empfänger zu senden.
- **Pager**. Mit dieser Methode können Sie eine Alarmmeldung an einen numerischen oder alphanumerischen Pager übermitteln.
- **Protokollierung**. Diese Methode weist den Windows-Ereignisprotokollierdienst an, jedes Virusentdeckungsereignis in der Windows-Ereignisanzeige festzuhalten. Diese Methode ist standardmäßig aktiviert. Die Windows-Ereignisanzeige, die sich auf dem Computer befindet, auf dem Warnungs-Manager installiert ist, empfängt die Benachrichtigung, nachdem der Scanner ein Virus entdeckt hat.
- **Drucker**. Diese Methode sendet Alarmmeldungen direkt an die jeweils angegeben Druckerwarteschlange.
- **SNMP**. Diese Methode sendet eine Meldung an ein SNMP-Abfanganzeigeprogramm (SNMP = Simple Network Management Protocol), wie z.B. Hewlett-Packard OpenView.
- **DMI**. Diese Methode sendet eine Meldung direkt an das Desktop Management Interface (sofern dieses installiert ist).
- **Programm**. Diese Methode startet eine .EXE-Datei, sobald der Scanner ein Virus entdeckt hat.
- **Ton**. Diese Methode startet eine .WAV-Datei, sobald der Scanner ein Virus entdeckt hat.
- **Terminal Server**. Diese Methode sendet eine Meldung an den Terminal Server-Client, der die Alarmmeldung erzeugt hat. Diese Warnmethode ist nur verfügbar, wenn die Virenschutzsoftware das Vorhandensein von Terminal Server entdeckt.

Zusätzlich zu diesen Warnmethoden gibt es eine weitere Registerkarte, die mit Zentrale Warnung beschriftet ist. Mit dieser Registerkarte können Sie das Dienstprogramm Warnungs-Manager so konfigurieren, daß es Alarmmeldungen liest und verteilt, die von McAfee GroupShield für Exchange erstellt wurden. Damit diese Methode genutzt werden kann, muß jede Installation von GroupShield für Exchange so eingerichtet und konfiguriert sein, daß sie Meldungen an den Ordner sendet, den Sie als Sammelpunkt für Viruswarnungen festgelegt haben. Benutzer müssen *Schreibrechte* für den Ordner für Viruswarnungen haben.

❑ **ANMERKUNG:** Wenn Sie Warnungs-Manager als Ressource in einem Cluster verwenden, muß sich der Ordner, in dem die Alarmmeldungen gesammelt werden, auf dem freigegebenen Datenträger des Clusters befinden.

Diese Methode kann auch von McAfee VirusScan für Windows NT verwendet werden, das auf einer Windows NT 4.0- oder Windows 2000 Professional-Arbeitsstation ausgeführt wird. Wahrscheinlich ist für diesen Zweck aber die Methode **Weiterleiten** besser geeignet.

Klicken Sie auf die Registerkarte, die der Warnmethode entspricht, die Sie konfigurieren möchten. Es werden die verfügbaren Optionen angezeigt. Nachdem Sie die Optionen wie gewünscht eingestellt haben, klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, ohne daß das Dialogfeld Warnungs-Manager geschlossen wird. Wenn Sie die Änderungen speichern und das Dialogfeld schließen möchten, klicken Sie auf **OK**. Wenn Sie das Dialogfeld schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**. Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Wie viele Warnungs-Manager sind erforderlich?

Sobald das Dienstprogramm Warnungs-Manager auf einem Windows NT- oder Windows 2000-Server installiert wurde, kann es Informationen vom Scanner bei Zugriff, vom Scanner auf Anforderung, vom AutoUpdate-Modul und von Arbeitsstationen des Netzwerks empfangen, die die Methode „Zentrale Warnung“ verwenden. Üblicherweise genügt eine Instanz von Warnungs-Manager, um vollständige Benachrichtigungsdienste bereitzustellen.

Es kann Situationen geben, in denen es vorteilhaft ist, mehrere funktionierende Instanzen von Warnungs-Manager zu haben. Zum Beispiel könnten Sie vorsehen, daß jeder Geschäftsbereich eine andere Instanz von Warnungs-Manager verwendet. Die Lösung für dieses Szenario besteht darin, Warnungs-Manager mehrfach zu installieren. Sie müssen die Instanzen von Warnungs-Manager auf unterschiedlichen Servern installieren. Diese Server könnten ein lokaler Server und ein entfernter Server (Remote-Server) des Netzwerks oder zwei entfernte Server sein. In Active Directory können eine oder mehrere Instanzen von Warnungs-Manager angemeldet werden.

Öffnen der Registerkarten von Warnungs-Manager

Verwenden Sie die Registerkarte **Warnungen**, um McAfee Warnungs-Manager zu starten. Warnungs-Manager verwendet eine Reihe von Benachrichtigungen, die für GroupShield für Exchange spezifisch sind und von Warnmethoden Ihrer Wahl gesendet werden, um Administratoren z.B. über einen Virusangriff oder fehlgeschlagene Systemtasks zu benachrichtigen.

Führen Sie folgende Schritte aus, um die Registerkarte Warnungen anzuzeigen und Warnungs-Manager zu starten:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Warnungen.
2. Aktivieren Sie im Feld Warnungen das Kontrollkästchen **Warnungs-Manager/Virenschutzinformant aktivieren**.

   Wenn Sie das Dienstprogramm Warnungs-Manager nicht verwenden, werden Administratoren über eine E-Mail-Nachricht über einen Virusangriff informiert (wie auf der Registerkarte Benachrichtigung beschrieben). Sie müssen jedoch dieses Kontrollkästchen aktiviert lassen, damit das McAfee-Dienstprogramm Virenschutzinformant seine Berichte senden kann. In der McAfee E-Policy Orchestrator-Dokumentation finden Sie Einzelheiten über das Virenberichttool Virenschutzinformant.
3. Klicken Sie im Feld Warnungs-Manager auf **Warnung**, um Warnungs-Manager zu starten.

   Beschreibungen, wie mit Warnungs-Manager gearbeitet werden kann, finden Sie in “Konfigurieren von Warnungs-Manager“ auf Seite 145.

❑ **ANMERKUNG:** Das Windows NT-Menü **Start** enthält für den lokalen Computer Verknüpfungen zu den Registerkarten von Warnungs-Manager. Führen Sie folgende Schritte aus, um die Registerkarten der lokalen Instanz von Warnungs-Manager zu öffnen:

a. Zeigen Sie im Menü **Start** auf **Programme**, und zeigen Sie dann auf **Network Associates**.

b. Wählen Sie aus dem Untermenü den Befehl **Warnungs-Manager-Konfiguration**.

   Es werden die Registerkarten von Warnungs-Manager angezeigt, wobei die Seite Zusammenfassung der Instanz von Warnungs-Manager, die auf dem lokalen Computer installiert ist, als oberste Seite angezeigt wird. (Siehe Abbildung 8-8 auf Seite 146).

Ergänzende Informationen

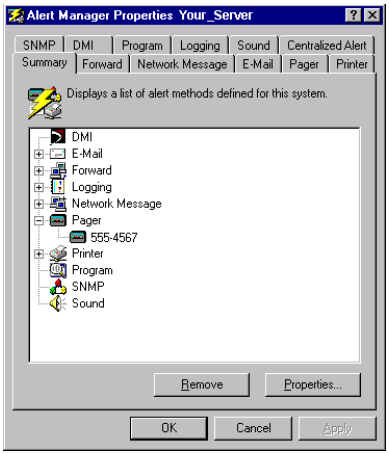
- Klicken Sie auf der Registerkarte Warnungen auf **Warnungen bearbeiten**, wenn Sie die Priorität oder den Inhalt einer Alarmmeldung ändern möchten. Weitere Informationen über das Ändern von Alarmmeldungen finden Sie im folgenden Abschnitt, “Ändern der Priorität einer Alarmmeldung”.

Konfigurieren von Warnungs-Manager

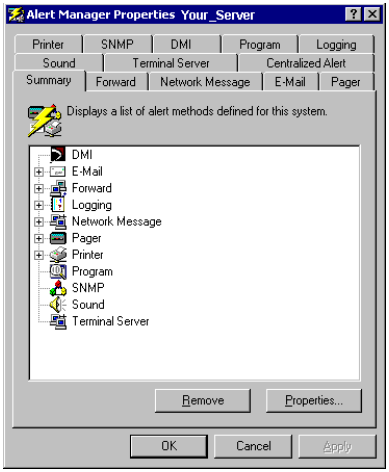
Jede Methode, mit der Warnungen gesendet werden können, wird durch eine Registerkarte repräsentiert. Klicken Sie auf die Registerkarte der Methode, die Sie verwenden möchten. In den folgenden Abschnitten sind alle Registerkarten und die für jede Methode verfügbaren Optionen beschrieben.

Anzeigen der Seite „Zusammenfassung“

Auf der Seite Zusammenfassung von Warnungs-Manager werden alle Warnmethoden aufgelistet, die Sie für den Einsatz konfiguriert haben. Das Fenster, das auf der *linken Seite* von Abbildung 8-8 auf Seite 146 abgebildet ist, zeigt das typische Aussehen der Registerkarten, wenn Warnungs-Manager auf einem Server installiert wurde, der kein Terminal Server ist. Wenn eine Instanz von Warnungs-Manager erkennt, daß sie auf einem Terminal Server installiert ist, wird zusätzlich die Registerkarte Warnungen angezeigt (siehe das Fenster auf der *rechten Seite* von Abbildung 8-8 auf Seite 146). Über diese Registerkarte können Sie das Benachrichtigungssystem für die Terminal Server-Clients aktivieren.



Terminal Server nicht entdeckt



Terminal Server entdeckt

Abbildung 8-8. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „Zusammenfassung“

Wenn Sie Warnungs-Manager noch nicht konfiguriert haben, enthält die Seite Zusammenfassung nur **Netzwerkmeldung** und **Protokollierung**. Dies sind die beiden Dienste, die standardmäßig aktiviert sind.

Klicken Sie auf ⊞ neben jeder aufgelisteten Warnmethode, damit die Ziele oder Zielgeräte angezeigt werden, an die Warnungs-Manager Meldungen übermittelt. Um eine Warnmethode zu entfernen, markieren Sie sie und klicken auf **Entfernen.** Um die Konfigurationsoptionen für eine aufgelistete Methode zu ändern, markieren Sie sie und klicken auf **Eigenschaften.** Warnungs-Manager öffnet dieselbe Registerkarte, mit der Sie auch die Optionen für diese Warnmethode konfiguriert haben.

In den folgenden Abschnitten wird erläutert, wie Sie die Optionen für jede Methode einstellen können.

WICHTIG: Um Warnungs-Manager auf einem Clusterserver zu konfigurieren, müssen Sie zunächst feststellen, auf welchem Server Warnungs-Manager momentan ausgeführt wird. Danach nehmen Sie die Konfiguration für diese Warnungs-Manager-Instanz vor. In einer Failover-Situation wird die Konfiguration von dem Knoten, auf dem Sie die Konfiguration vorgenommen haben, auf den anderen Knoten übertragen.

Weiterleiten von Alarmmeldungen an andere Computer

Warnungs-Manager kann die von einem Scanner erstellten Alarmmeldungen an einen anderen Computer in derselben Domäne weiterleiten, um die Alarmmeldungen in der Domäne weiter zu verteilen. In einem großen Unternehmen können Sie die Weiterleitungsfunktion verwenden, um Warnungen an ein zentrales Benachrichtigungssystem oder an eine MIS-Abteilung (MIS = Management-Informationssystem) zu senden, damit Virenstatistiken und Problembereiche ausgewertet werden können.

Das folgende Szenario dient als Beispiel, das die Nützlichkeit dieser Methode verdeutlicht:

> Sie möchten alle Alarmmeldungen mit hoher Priorität, die irgendein Server erstellt hat, an einen bestimmten Pager senden, aber nur ein Server hat ein Modem. Um dieser Anforderung gerecht zu werden:
>
> - Konfigurieren Sie die Instanz von Warnungs-Manager auf jedem Server so, daß sie Alarmmeldungen, die eine hohe Priorität haben, an den Computer in derselben Domäne weiterleitet, der mit einem Modem ausgerüstet ist.
> - Konfigurieren Sie die Instanz von Warnungs-Manager auf dem Computer mit Modem so, daß sie Meldungen, die eine hohe Priorität haben, an den Zielpager sendet.

ANMERKUNG: Informationen über das Senden von Warnungen an Pager siehe “Senden von Alarmmeldungen an Pager“ auf Seite 158. Informationen über das Angeben der Prioritätsstufe, die für Pagerwarnungen in Frage kommt, siehe Schritt 6 auf Seite 161. Informationen über das Einstellen von Prioritäten siehe “Anpassen von Alarmmeldungen“ auf Seite 182.

Gehen Sie zum Konfigurieren von Warnungs-Manager-Weiterleitungsoptionen wie folgt vor:

1. öffnen Sie die Registerkarten von Warnungs-Manager. Weitere Informationen siehe “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.
2. klicken Sie auf die Registerkarte Weiterleiten. Es wird die Seite Weiterleiten mit einer Liste aller Computer angezeigt, für die Sie festgelegt haben, daß sie weitergeleitete Meldungen empfangen sollen (siehe Abbildung 8-9 auf Seite 148).

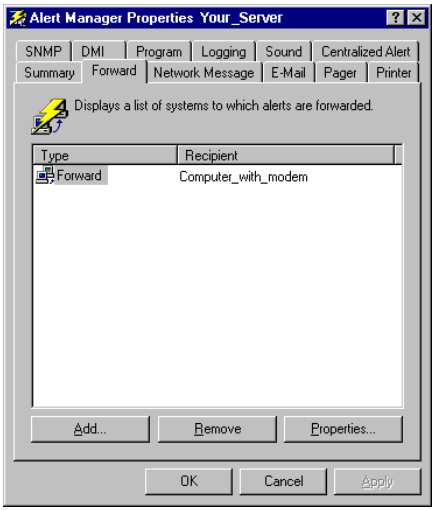


Abbildung 8-9. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „Weiterleiten“

3. Sie können diese Liste wie folgt aktualisieren:

   - **Einen Computer aus der Liste entfernen.** Wählen Sie einen der aufgelisteten Zielcomputer aus, und klicken Sie dann auf **Entfernen.**

   - **Einen Computer zur Liste hinzufügen.** Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Weiterleitungseigenschaften** (Abbildung 8-10 auf Seite 149) anzuzeigen. Geben Sie dann in das Textfeld den Namen des Computers ein, der die weitergeleiteten Meldungen empfangen soll. Sie können den Computernamen in UNC (Universal Naming Convention)-Notation eingeben oder auf **Durchsuchen** klicken, um den Computer im Netzwerk zu suchen. Fahren Sie mit Schritt 4 fort.

   - **Konfigurationsoptionen ändern.** Wählen Sie einen der aufgelisteten Zielcomputer aus, und klicken Sie dann auf **Eigenschaften.** Das Dialogfeld Weiterleitungseigenschaften wird angezeigt (siehe Abbildung 8-10). Ändern Sie die Informationen im Textfeld Computer. Fahren Sie mit Schritt 4 fort.

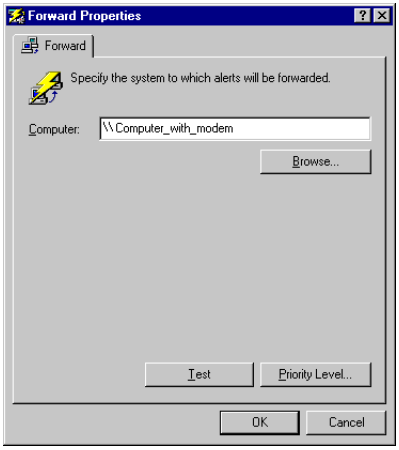


Abbildung 8-10. Dialogfeld „Weiterleitungseigenschaften“

4. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmmeldungen an den Zielcomputer gesendet werden sollen.

   Ziehen Sie im Dialogfeld **Prioritätsstufe** (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, damit weniger Meldungen, die eine entsprechend hohe Priorität haben, an den Zielcomputer gesendet werden. Wenn der Schieberegler sich ganz rechts befindet, werden nur Meldungen des Typs „Kritisch“ an den Zielcomputer gesendet.

   Ziehen Sie den Schieberegler nach links, damit mehr Alarmmeldungen gesendet werden, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, werden sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ gesendet.

   Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

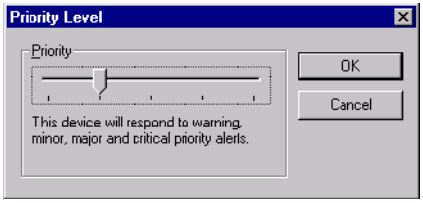


Abbildung 8-11. Das Dialogfeld „Prioritätsstufe“

5. Klicken Sie auf **Testen**, um eine Testmeldung an den Zielcomputer zu senden. Die Meldung wird auf dem Bildschirm des Zielcomputers in einem Dialogfeld angezeigt. Der Empfänger muß auf **OK** klicken, um die Meldung zu bestätigen.

   ANMERKUNG: Für den Fall, daß der Zielcomputer die Meldung nicht empfängt, öffnen Sie die Windows NT- oder Windows 2000-Ereignisanzeige und suchen nach einer Fehlermeldung. Wenn Sie keine entsprechende Fehlermeldung finden, gehen Sie die unten gezeigte Liste durch und überprüfen Sie die folgende Punkte:

   - Der zur Implementierung der ausgewählten Warnmethode erforderliche Kommunikationsdienst, wie z. B. E-Mail oder SNMP, ist aktiviert.
   - Das zur Übertragung oder zum Empfang der Meldung erforderliche Gerät, wie z. B. ein Modem oder Pager, ist vorhanden und betriebsbereit.
   - Das verwendete Systemkonto oder Benutzerkonto hat die erforderlichen Zugriffsrechte auf die Zielnetzwerkressource.
   - Das Kennwort des Kontos ist nicht abgelaufen.
   - Jede Datei, die als Reaktion auf eine Viruserkennung aktiviert werden soll, wie z. B. eine .EXE-, .BAT- oder .WAV-Datei, befindet sich im angegebenen Pfad und funktioniert ordnungsgemäß.
   - Der als Ziel dienende Drucker, Benutzer oder Computer ist im Netzwerk vorhanden.
   - Ihr Netzwerk funktioniert ordnungsgemäß.
   - Die von Ihnen eingegebenen Konfigurationsdaten sind richtig und vollständig. Einige Registerkarten enthalten untergeordnete Seiten. So führt z. B. die Seite E-Mail-Eigenschaften zu einer Seite Mail-Einstellungen; die Seite Pager-Eigenschaften führt zu einer Seite Modemeinstellungen. Achten Sie darauf, auch die Informationen auf diesen untergeordneten Seiten zu überprüfen.

   Wenn Sie die ausgewählte Warnungs-Manager-Methode trotzdem nicht erfolgreich testen können, finden Sie unter “Technischer Support“ auf Seite xix Informationen, wie Sie zusätzliche Unterstützung finden.

6. Klicken Sie auf **OK**, um zum Dialogfeld Warnungs-Manager-Eigenschaften zurückzukehren.

7. Wenn Sie die Konfigurationsoptionen speichern und das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, klicken Sie auf **OK.** Wenn Sie die Änderungen speichern und das Konfigurieren von Warnungs-Manager fortsetzen möchten, klicken Sie auf **Übernehmen** und dann auf eine andere Registerkarte. Wenn Sie das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen.** Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Senden einer Alarmmeldung als Netzwerkmeldung

Warnungs-Manager kann die Alarmmeldungen, die der Scanner erstellt, mit einer standardmäßigen Windows NT 4.0- oder Windows 2000-Netzwerk-Broadcast-Meldung an andere Computer oder Benutzer des Netzwerks senden. Die jeweilige Warnmeldung wird auf dem Bildschirm des Zielcomputers angezeigt und verlangt vom Empfänger, daß er sie bestätigt.

ACHTUNG: Ein Benutzer kann gleichzeitig bei mehreren Computern angemeldet sein, aber Computernamen müssen im Netzwerk eindeutig sein. Daher ist ein Benutzer kein so zuverlässiges Benachrichtigungsziel wie ein Zielcomputer.

Auf Zielcomputern muß der Nachrichtendienst von Windows NT 4.0 oder Windows 2000 ausgeführt werden, damit Alarmmeldungen empfangen werden können. Auf Zielcomputern, die unter Windows 95 oder Windows 98 arbeiten, muß das Dienstprogramm WinPopup ausgeführt werden, damit Alarmmeldungen empfangen werden können. WinPopup ist in einigen Windows-Versionen enthalten. Einzelheiten finden Sie in Ihrer Windows-Dokumentation.

TIP: Wenn Sie Terminal Server als Warnmethode verwenden, empfiehlt McAfee, daß Sie als Methode für das Senden von Meldungen keine Netzwerkmeldung verwenden. Normalerweise wird die Terminal Server-Methode verwendet, um Alarmmeldungen an den Computer zu senden, der die Alarmmeldung erstellt hat. Bei der Netzwerkmeldungsmethode wird eine Meldung an alle Terminal Server-Clients gesendet. Weitere Informationen über Terminal Server finden Sie unter “Senden einer Alarmmeldung an Terminal Server-Clients“ auf Seite 177.

Um Alarmmeldungen als Netzwerkmeldungen zu senden, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.

2. Klicken Sie auf die Registerkarte Netzwerkmeldung.

   Die Registerkarte Netzwerkmeldung wird angezeigt. Auf dieser Seite wird eine Liste der Computer oder Benutzernamen angezeigt, die Sie als Ziele für Netzwerkmeldungen festgelegt haben (Abbildung 8-12 auf Seite 152). Wenn Sie noch keinen Zielcomputer oder -Benutzer gewählt haben, ist diese Liste leer.

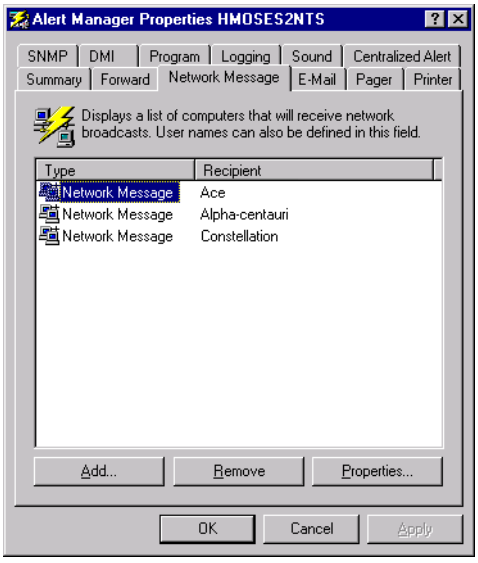


Abbildung 8-12. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „Netzwerkmeldung“

3. Sie können diese Liste wie folgt aktualisieren:

   - **Einen Computer oder Benutzer aus der Liste entfernen**. Wählen Sie einen der aufgelisteten Zielcomputer oder Empfängernamen aus, und klicken Sie dann auf **Entfernen**.
   - **Einen Computer oder Benutzer zur Liste hinzufügen.** Klicken Sie auf **Hinzufügen**, um das Dialogfeld Netzwerkmeldungseigenschaften (Abbildung 8-13 auf Seite 153) anzuzeigen. Geben Sie dann in das Textfeld den Namen des Empfängers oder Zielcomputers ein. Sie können den Computernamen in UNC (Universal Naming Convention)-Notation eingeben oder auf **Durchsuchen** klicken, um den Computer im Netzwerk zu suchen. Fahren Sie danach mit Schritt 4 fort.

- **Konfigurationsoptionen ändern.** Wählen Sie einen der aufgelisteten Zielcomputer oder Empfängernamen aus, und klicken Sie dann auf **Eigenschaften**. Das Dialogfeld Netzwerkmeldungseigenschaften wird angezeigt (Abbildung 8-13 auf Seite 153). Ändern Sie die Informationen im Textfeld **Computer**. Fahren Sie danach mit Schritt 4 fort.

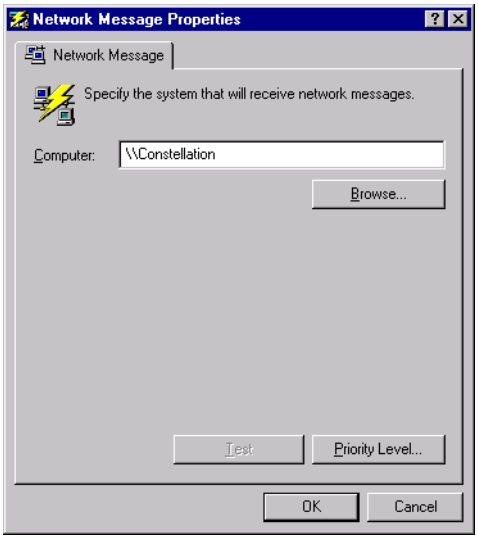


Abbildung 8-13. Dialogfeld „Netzwerkmeldungseigenschaften“

4. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmmeldungen an den Zielcomputer oder -benutzer gesendet werden sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, damit weniger Meldungen, die eine entsprechend hohe Priorität haben, an die angegebenen Computer gesendet werden. Wenn der Schieberegler sich ganz rechts befindet, werden nur Meldungen des Typs „Kritisch“ an die von Ihnen angegebenen Computer gesendet.

   Ziehen Sie den Schieberegler nach links, damit mehr Alarmmeldungen gesendet werden, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, werden sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ gesendet.

   Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

5. Klicken Sie auf **Testen**, um eine Testmeldung an den Zielcomputer oder -benutzer zu senden.

   Die Meldung wird auf dem Bildschirm des Zielcomputers in einem Dialogfeld angezeigt. Der Empfänger muß auf **OK** klicken, um die Meldung zu bestätigen. Wenn die Meldung nicht beim Empfänger ankommt:

   - Überprüfen Sie die Punkte, die in der **Anmerkung** auf Seite 150 aufgeführt sind.
   - Suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige nach einer Fehlermeldung.

6. Klicken Sie auf **OK**, um zur Seite Netzwerkmeldung zurückzukehren.
7. Wenn Sie die Konfigurationsoptionen speichern und das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, klicken Sie auf OK. Wenn Sie die Änderungen speichern und das Konfigurieren von Warnungs-Manager fortsetzen möchten, klicken Sie auf **Übernehmen** und dann auf eine andere Registerkarte. Wenn Sie das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**. Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Senden von Alarmmeldungen an E-Mail-Adressen

Warnungs-Manager kann die Alarmmeldungen, die der Scanner erstellt, über Standard-SMTP-E-Mail-Dienste (SMTP = Simple Mail Transfer Protocol) an die E-Mail-Adresse eines Empfängers senden. Die Alarmmeldungen werden im Postfach des Empfängers abgelegt. Wenn die Meldung besonders dringend ist, sollten Sie die entsprechende E-Mail-Nachricht durch andere Methoden unterstützen, damit gewährleistet ist, daß der Empfänger die Alarmmeldung rechtzeitig sieht, um eine geeignete Aktion zu unternehmen.

Um Alarmmeldungen als E-Mail-Nachrichten zu senden, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.
2. Klicken Sie auf die Registerkarte E-Mail.

   Es wird die Seite E-Mail mit einer Liste aller E-Mail-Adressen angezeigt, für die Sie festgelegt haben, daß sie Alarmmeldungen empfangen sollen (siehe Abbildung 8-14). Wenn Sie noch keine E-Mail-Adresse angegeben haben, ist diese Liste leer.

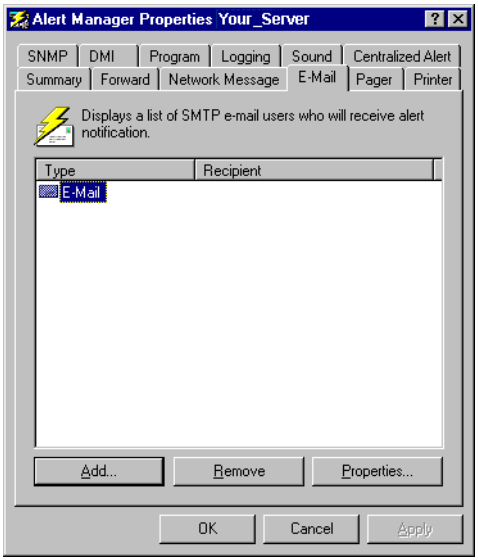


Abbildung 8-14. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „E-Mail“

3. Sie können diese Liste wie folgt aktualisieren:

   - **Eine Adresse aus der Liste entfernen.** Wählen Sie eine der aufgelisteten E-Mail-Adressen aus, und klicken Sie dann auf **Entfernen.**

   - **Eine E-Mail-Adresse zur Liste hinzufügen.** Klicken Sie auf **Hinzufügen**, um das Dialogfeld E-Mail-Eigenschaften anzuzeigen (Abbildung 8-15). Geben Sie die E-Mail-Adresse des Empfängers in das Textfeld Adresse, den Betrefftext in das Textfeld Betreff und Ihre E-Mail-Adresse in das Textfeld Von ein. Verwenden Sie das Standardformat für Internet-Adressen: *<benutzername>@<domäne>* (z.B. admin@meinedomäne.com). Fahren Sie danach mit Schritt 4 fort.

   - **Konfigurationsoptionen ändern.** Wählen Sie eine der aufgelisteten E-Mail-Adressen aus, und klicken Sie dann auf **Eigenschaften.** Das Dialogfeld E-Mail-Eigenschaften wird angezeigt (siehe Abbildung 8-15). Ändern Sie die in den angezeigten Textfeldern enthaltenen Informationen, die Sie ändern möchten. Fahren Sie danach mit Schritt 4 fort.

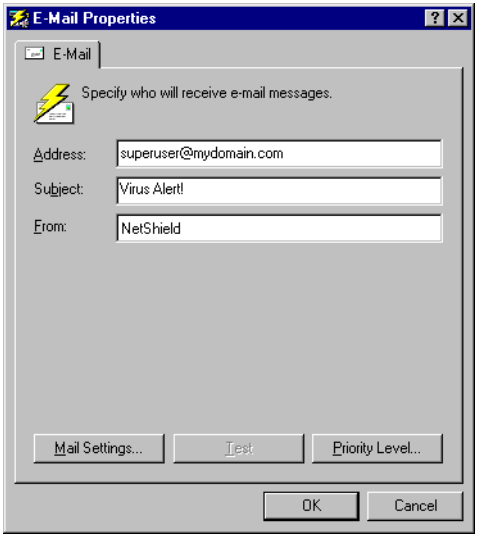


Abbildung 8-15. Das Dialogfeld „E-Mail-Eigenschaften“

4. Klicken Sie auf **Mail-Einstellungen**, um den SMTP-Server anzugeben, der Internet-Mail sendet. Geben Sie im daraufhin angezeigten Dialogfeld (siehe Abbildung 8-16 auf Seite 156) in das Textfeld Server den Namen des Servers und in das Textfeld Anmeldung den Benutzernamen eines aktiven E-Mail-Kontos ein, das die Scansoftware verwenden kann, um sich beim Server anzumelden.

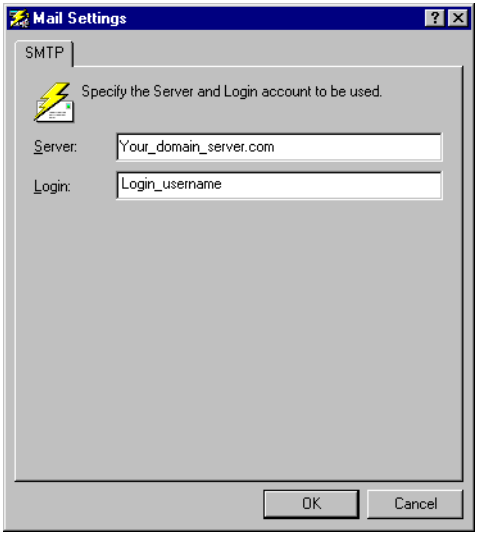


Abbildung 8-16. Das Dialogfeld „Mail-Einstellungen“

Sie können den Servernamen als IP-Adresse (IP = Internet Protocol), als Namen, den der lokale DNS-Server erkennt, als NetBIOS-Namen, als WINS-Namen (WINS = Windows Internet Name Service) oder in der UNC-Schreibweise (UNC = Universal Naming Convention) eingeben.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern und zum Dialogfeld E-Mail-Eigenschaften zurückzukehren.

6. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmmeldungen an den Empfänger gesendet werden sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, damit weniger Meldungen, die eine entsprechend hohe Priorität haben, per E-Mail gesendet werden. Wenn der Schieberegler sich ganz rechts befindet, werden nur Meldungen des Typs „Kritisch“ per E-Mail gesendet.

   Ziehen Sie den Schieberegler nach links, damit mehr Alarmmeldungen gesendet werden, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, werden sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ gesendet.

   Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

7. Klicken Sie auf **Testen**, um eine Testmeldung als Nachricht an die E-Mail-Adresse zu senden, die Sie eingegeben haben. Die Nachricht wird im Postfach des Empfängers abgelegt. Wenn die Meldung nicht beim Empfänger ankommt:

   - Überprüfen Sie die Punkte, die im Hinweis auf Seite 150 aufgeführt sind.
   - Suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige nach einer Fehlermeldung.

8. Klicken Sie auf **OK**, um zur Seite E-Mail zurückzukehren.

9. Um andere Benachrichtigungsoptionen zu konfigurieren, klicken Sie auf eine andere Registerkarte. Wenn Sie die Konfigurationsoptionen speichern und das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, klicken Sie auf **OK**. Wenn Sie die Änderungen speichern und das Konfigurieren von Warnungs-Manager fortsetzen möchten, klicken Sie auf **Übernehmen** und dann auf eine andere Registerkarte. Wenn Sie das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen.** Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Senden von Alarmmeldungen an Pager

Warnungs-Manager kann Alarmmeldungen, die der Scanner erstellt hat, an den Pager eines Empfängers senden. Dies setzt allerdings voraus, daß der Server, auf dem die Virenschutzsoftware ausgeführt wird, über ein Modem mit dem Telefonnetz verbunden ist.

TIP: Wenn es mehrere Server gibt, aber nur einer dieser Server über ein Modem mit dem Telefonnetz verbunden ist, können Sie Alarmmeldungen von allen Servern an den Server mit Modem weiterleiten, damit dieser die Meldungen an den Pager überträgt. Siehe “Weiterleiten von Alarmmeldungen an andere Computer“ auf Seite 147.

Warnungs-Manager unterstützt sowohl alphanumerische Pager als auch Pager, die nur numerische Meldungen empfangen. Möglicherweise müssen Sie für das Wählen oder das Angeben von Menüoptionen ein eigenes Skript schreiben, um den Verbindungsvorgang zum jeweiligen Pagerdienst zu erledigen.

Gehen Sie zum Senden von Alarmmeldungen an einen Pager wie folgt vor:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.

2. Klicken Sie auf die Registerkarte Pager.

   Es wird die Seite Pager (Abbildung 8-17 auf Seite 159) mit einer Liste aller Pagernummern angezeigt, für die Sie festgelegt haben, daß sie Alarmmeldungen empfangen sollen. Wenn Sie noch keine Pagernummer angegeben haben, ist diese Liste leer.

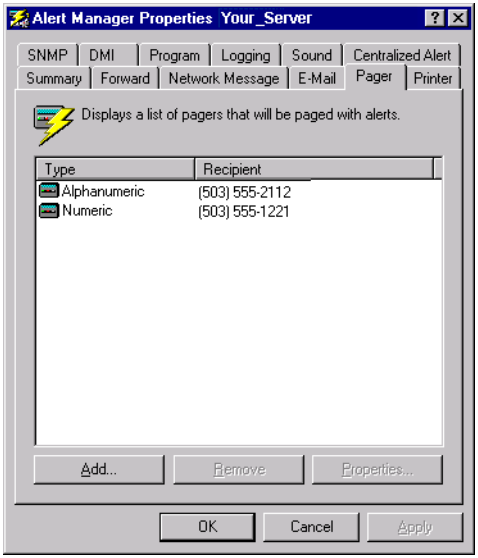


Abbildung 8-17. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „Pager“

3. Sie können diese Liste wie folgt aktualisieren:

   - **Eine Pagernummer aus der Liste entfernen.** Wählen Sie eine der aufgelisteten Pagernummern aus, und klicken Sie dann auf **Entfernen.**
   - **Eine Pagernummer zur Liste hinzufügen.** Klicken Sie auf **Hinzufügen**, um das Dialogfeld Pager-Eigenschaften anzuzeigen (siehe Abbildung 8-18 auf Seite 160). Wählen Sie in der Liste oben auf der Seite den Pagertyp aus, den der Empfänger hat, und geben Sie die Informationen für diesen Pagertyp in die entsprechenden Textfelder ein.

     – Wenn der Empfänger einen alphanumerischen Pager verwendet, geben Sie die Pagernummer und, sofern erforderlich, die ID und das Kennwort des Empfängers ein. Aktivieren Sie anschließend die Option **Alarmmeldung verwenden**, um die Standardalarmmeldung zu senden, oder aktivieren Sie die Option **Eigene Meldung verwenden**, und geben Sie dann Ihre eigene Meldung in das Textfeld ein.

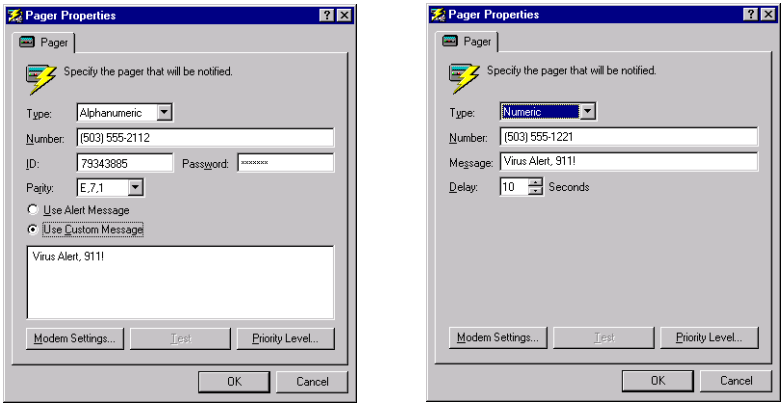
       Die Telefonnummer für das Senden einer alphanumerischen Pagermeldung per Modem ist eventuell nicht die Nummer, die eine Person wählen muß, um eine Nachricht auf dem Pager zu hinterlassen. Die korrekte Konfiguration erfahren Sie vom Anbieter des Pagerdienstes.

Wenn Alarmmeldung verwenden aktiviert ist, wird eine Standardmeldung gesendet, die das jeweilige Ereignis beschreibt, das Ursache der Alarmmeldung war. Wenn Eigene Meldung verwenden aktiviert ist, wird eine unveränderliche benutzerdefinierte Meldung gesendet, und zwar unabhängig davon, welches Ereignis die Alarmmeldung ausgelöst hat.

– Wenn der Empfänger einen numerischen Pager verwendet, geben Sie in die entsprechenden Textfelder die Pagernummer und die numerische Meldung ein, die gesendet werden soll. Geben Sie anschließend in das Feld **Verzögerung** einen Wert ein, der angibt, wie viele Sekunden Warnungs-Manager zwischen dem Wählvorgang und dem Übermitteln einer Meldung warten soll. Räumen Sie Warnungs-Manager genügend Zeit ein, um die Anfangsbegrüßung sowie weitere vorbereitende Meldungen abzuwarten, die der Pagerdienst sendet, bevor er Meldungen entgegennimmt. Für den Fall, daß der Dienst Tastentöne erwartet, um Menüoptionen zu aktivieren, müssen Sie eventuell ein Anmeldeskript schreiben, das für das Modem verwendet wird.

Fahren Sie mit Schritt 4 fort.

- **Konfigurationsoptionen ändern.** Wählen Sie eine der aufgelisteten Pagernummern aus, und klicken Sie dann auf **Eigenschaften.** Das Dialogfeld Pager-Eigenschaften wird angezeigt (Abbildung 8-18). Ändern Sie die in den angezeigten Textfeldern enthaltenen Informationen, die Sie ändern möchten. Fahren Sie mit Schritt 4 fort.



Alphanumerischer Pager **Numerischer Pager**

Abbildung 8-18. Dialogfeld „Pager-Eigenschaften“

4. Klicken Sie auf **Modemeinstellungen**, um das Modem so zu konfigurieren, daß es Pagermeldungen senden kann. Geben Sie im Dialogfeld, das angezeigt wird (Abbildung 8-19 auf Seite 161), folgendes an: in der Liste Modem den Typ des Modems, das an den Server angeschlossen ist; in der Liste Anschluß den COM-Anschluß für das Modem; und in der Liste Baud die Datenrate, mit das Modem Daten übertragen kann. Geben Sie dann in die entsprechenden Textfelder eventuell erforderliche Vorwahlen oder Nummernsuffixe ein, die das Modem wählen muß, um Amtsleitungen zu erreichen, bestimmte Netzbetreiber für Fernleitungen zu verwenden, persönliche Identifikationsnummern anzugeben oder ähnliche Aufgaben zu erledigen.

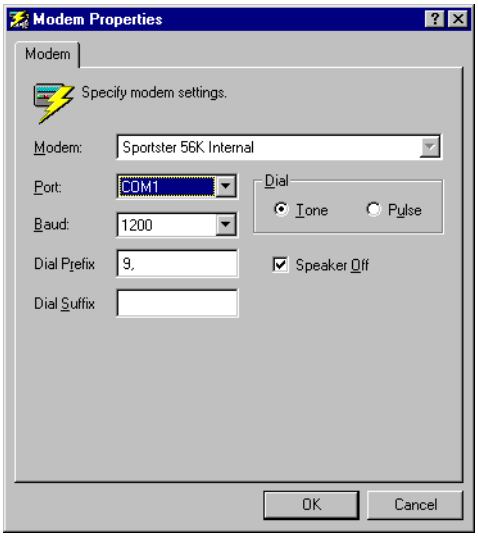


Abbildung 8-19. Dialogfeld „Modemeigenschaften“

Aktivieren Sie die Wählmethode (**Ton** oder **Impuls**), die das Modem verwenden soll, und aktivieren Sie das Kontrollkästchen Lautsprecher, wenn das Modem tonlos wählen und verbinden soll.

5. Klicken Sie auf **OK**, um die Einstellungen zu speichern und zum Dialogfeld Pager-Eigenschaften zurückzukehren.

6. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmmeldungen an den Pager gesendet werden sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, damit weniger Nachrichten und nur noch solche ab einer bestimmten Prioritätsstufe an den Pager gesendet werden. Wenn der Schieberegler sich ganz rechts befindet, werden nur Meldungen des Typs „Kritisch“ an den Pager gesendet.

Ziehen Sie den Schieberegler nach links, damit mehr Alarmmeldungen gesendet werden, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, werden sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ gesendet.

Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

7. Klicken Sie auf **Testen**, um eine Testmeldung an die eingegebene Pagernummer zu senden. Wenn der Empfänger einen alphanumerischen Pager hat, erhält er vom Warnungs-Manager eine Textmeldung. Wenn der Empfänger einen numerischen Pager hat, wird auf diesem die Telefonnummer oder andere Meldung, die Sie im Dialogfeld Pager-Eigenschaften angegeben haben, angezeigt. Wenn die Meldung nicht beim Empfänger ankommt:

   - Überprüfen Sie die Punkte, die im Hinweis auf Seite 150 aufgeführt sind.
   - Suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige nach einer Fehlermeldung.

8. Klicken Sie auf **OK**, um die Änderungen zu speichern und zur Seite Pager zurückzukehren.

9. Wenn Sie die Konfigurationsoptionen speichern und das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, klicken Sie auf **OK**. Wenn Sie die Änderungen speichern und das Konfigurieren von Warnungs-Manager fortsetzen möchten, klicken Sie auf **Übernehmen** und dann auf eine andere Registerkarte. Wenn Sie das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen.** Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Senden von Alarmmeldungen an einen Drucker

Warnungs-Manager kann Alarmmeldungen, die der Scanner erstellt hat, an Drucker oder Druckserver als Druckauftrag zur Verarbeitung schicken. Damit Sie diese Option nutzen können, müssen Sie zunächst den Drucker einrichten und den korrekten Druckertreiber wählen. Ausführlichere Informationen finden Sie in der Dokumentation von Microsoft Windows NT 4.0 oder Microsoft Windows 2000.

Um den Warnungs-Manager so zu konfigurieren, daß er Alarmmeldungen an einen Drucker sendet, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.

2. Klicken Sie auf die Registerkarte Drucker. Es wird die Seite Drucker (Abbildung 8-20 auf Seite 163) mit einer Liste aller Drucker angezeigt, die Sie installiert haben. Wenn Sie noch keinen Drucker angegeben haben, ist diese Liste leer.

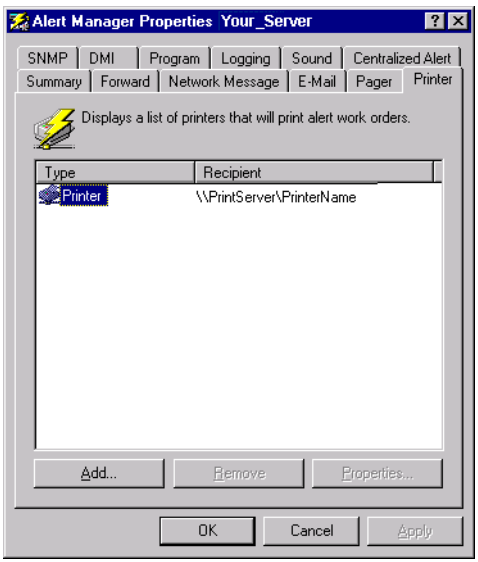


Abbildung 8-20. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „Drucker“

3. Sie können diese Liste wie folgt aktualisieren:

   - **Einen Drucker aus der Liste entfernen.** Wählen Sie einen der aufgelisteten Drucker aus, und klicken Sie dann auf **Entfernen.**
   - **Einen Drucker zur Liste hinzufügen.** Klicken Sie auf **Hinzufügen**, um das Dialogfeld Druckereigenschaften anzuzeigen (siehe Abbildung 8-21 auf Seite 164). Geben Sie in das Textfeld den Namen des Zieldruckers ein, oder klicken Sie auf **Durchsuchen**, um den Drucker im Netzwerk zu suchen. Fahren Sie danach mit Schritt 4 fort.

- **Konfigurationsoptionen ändern.** Wählen Sie eine der aufgelisteten Durckerwarteschlangen aus, und klicken Sie dann auf **Eigenschaften.** Das Dialogfeld Druckereigenschaften wird angezeigt (Abbildung 8-21 auf Seite 164). Ändern Sie die Informationen im Textfeld Drucker. Fahren Sie danach mit Schritt 4 auf Seite 164 fort.

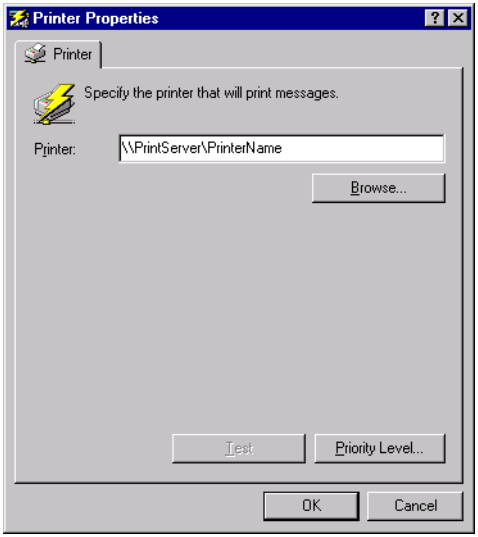


Abbildung 8-21. Dialogfeld “Druckereigenschaften“

4. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmmeldungen an den Zieldrucker gesendet werden sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, damit weniger Nachrichten und nur noch solche ab einer bestimmten Prioritätsstufe an den Drucker gesendet werden. Wenn der Schieberegler sich ganz rechts befindet, werden nur Meldungen des Typs „Kritisch“ an den Drucker gesendet.

   Ziehen Sie den Schieberegler nach links, damit mehr Alarmmeldungen gesendet werden, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, werden sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ gesendet.

   Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Ändern der Priorität einer Alarmmeldung“ auf Seite 184.

5. Klicken Sie auf **Testen**, um eine Testmeldung an den Zieldrucker zu senden. Mit dieser Meldung wird eine einfache unformatierte Textzeile gedruckt. Wenn der Drucker die Meldung nicht druckt:

   - Überprüfen Sie die Punkte, die im Hinweis auf Seite 150 aufgeführt sind.
   - Suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige nach einer Fehlermeldung.

6. Klicken Sie auf **OK**, um zur Seite **Drucker** zurückzukehren.

7. Wenn Sie die Konfigurationsoptionen speichern und das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, klicken Sie auf **OK**. Wenn Sie die Änderungen speichern und das Konfigurieren von Warnungs-Manager fortsetzen möchten, klicken Sie auf **Übernehmen** und dann auf eine andere Registerkarte. Wenn Sie das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen.**

   ANMERKUNG: Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Senden von Alarmmeldungen über SNMP

Warnungs-Manager kann von der Virenschutzsoftware generierte Meldungen mit Hilfe von SNMP (Simple Network Management Protocol) an andere Computer senden. Um diese Option verwenden zu können, müssen Sie den SNMP-Dienst und Warnungs-Manager auf demselben Server installieren.

TIP: Wenn Sie Warnungs-Manager vor der Installation des SNMP-Dienstes installieren, kann Warnungs-Manager nicht die von SNMP benötigten Registrierungsschlüssel erstellen. Um dieses Problem zu lösen, installieren Sie Warnungs-Manager nach der Installation des SNMP-Dienstes erneut. Starten Sie dann den SNMP-Dienst neu.

Um die vom Scanner gesendeten Alarmmeldungen anzeigen zu können, muß ein Netzwerkverwaltungssystem, wie z. B. Network Associates Event Orchestrator oder Hewlett-Packards OpenView, installiert und so konfiguriert sein, daß es die Management Information Base (.MIB)-Dateien von Warnungs-Manager in ein lesbares Format konvertiert. Diese Dateien, die die Namen ANTIVIRS.MIB und NAI.MIB haben, befinden sich in dem Ordner, in dem das Virenschutzprogramm installiert ist. Das Netzwerkverwaltungssystem kann sich an beliebiger Stelle im Netzwerk befinden. Konfigurationsinformationen finden Sie in der Dokumentation zu Ihrem Netzwerkverwaltungssystem.

Um die Warnungs-Manager-Instanz so zu konfigurieren, daß sie Alarmmeldungen über SNMP sendet, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.

2. Klicken Sie auf die Registerkarte SNMP.

   Die Registerkarte SNMP wird angezeigt (siehe Abbildung 8-22 auf Seite 166).

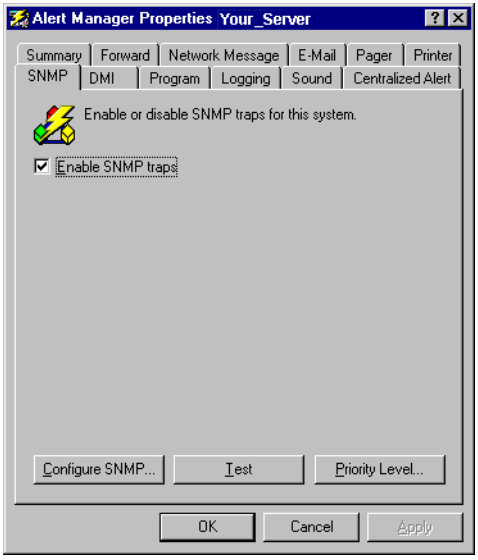


Abbildung 8-22. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „SNMP“

3. Aktivieren Sie das Kontrollkästchen **SNMP-Traps aktivieren**.

4. Um Alarmmeldungen über SNMP senden zu können, müssen Sie SNMP auf dem Server installieren und aktivieren. Wenn Sie diesen Dienst noch nicht konfiguriert haben, klicken Sie auf **SNMP konfigurieren**, um die Netzwerksteuerung zu starten. Das Aussehen der Netzwerksteuerung ist in Windows 2000 und Windows NT 4.0 leicht unterschiedlich. In beiden Fällen besteht Ihre Aufgabe darin, den SNMP-Dienst hinzuzufügen und dann zu konfigurieren. Möglicherweise müssen Sie in der Windows-Dokumentation nachlesen, um weitere Informationen zu erhalten, und die Installations-CDs des Betriebssystems zur Hand haben.

5. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmmeldungen an den SNMP-Verwaltungscomputer gesendet werden sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, damit weniger Meldungen, die eine entsprechend hohe Priorität haben, über SNMP gesendet werden. Wenn der Schieberegler sich ganz rechts befindet, werden nur Meldungen des Typs „Kritisch“ über SNMP gesendet.

   Ziehen Sie den Schieberegler nach links, damit mehr Alarmmeldungen gesendet werden, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, werden sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ gesendet.

   Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

6. Klicken Sie auf **Testen**, um eine Testmeldung an den SNMP-Computer zu senden. Wenn die Meldung nicht beim Empfänger ankommt:

   - Überprüfen Sie die Punkte, die im Hinweis auf Seite 150 aufgeführt sind.
   - Suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige nach einer Fehlermeldung.

7. Klicken Sie auf **OK**, um zur Seite SNMP zurückzukehren.

8. Wenn Sie die Konfigurationsoptionen speichern und das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, klicken Sie auf **OK**. Wenn Sie die Änderungen speichern und das Konfigurieren von Warnungs-Manager fortsetzen möchten, klicken Sie auf **Übernehmen** und dann auf eine andere Registerkarte. Wenn Sie das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen.**

❑ **ANMERKUNG:** Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Senden von Alarmmeldungen über Desktop Management Interface

Warnungs-Manager kann die Alarmmeldungen, die der Scanner erstellt hat, über die Ebene der DMI-Interfacekomponente (DMI = Desktop Management Interface) senden. DMI ist ein für mehrere Plattformen definierter Standard zum Übermitteln von Verwaltungsanforderungen und Alarminformationen zwischen Hardware- und Softwarekomponenten, die auf einem Desktopcomputer gespeichert oder an diesen angeschlossen sind, und den Anwendungen, mit denen die Komponenten verwaltet werden.

Damit Sie diese Warnmethode nutzen können, müssen Sie DMI-Verwaltungssoftware im Netzwerk installiert und konfiguriert haben. Ausführlichere Informationen finden Sie in der Dokumentation der DMI-Software.

ANMERKUNG: Wenn Sie mehr zu dem Desktop Management Interface-Standard wissen möchten, sollten Sie sich die Website Desktop Management Task Force unter http://www.dmtf.org ansehen.

Um die Warnungs-Manager-Instanz so zu konfigurieren, daß sie Alarmmeldungen über DMI sendet, führen Sie diese Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Informationen zur Vorgehensweise finden Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.
2. Klicken Sie auf die Registerkarte DMI.

   Die Registerkarte DMI (siehe Abbildung 8-23 auf Seite 168) wird angezeigt.

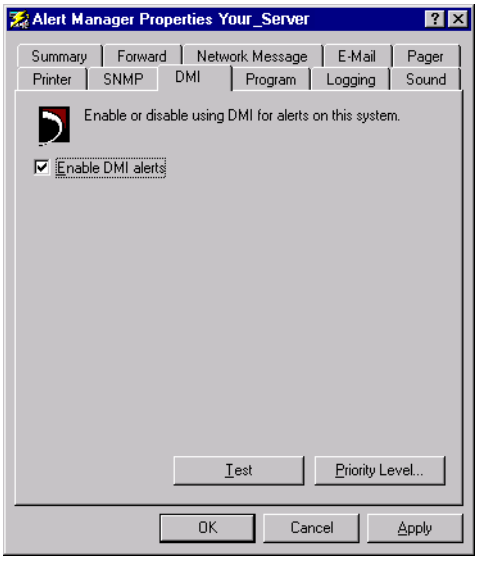


Abbildung 8-23. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „DMI“

3. Aktivieren Sie das Kontrollkästchen **DMI-Alarmmeldungen aktivieren**.

4. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmmeldungen an die DMI-Verwaltungssoftware gesendet werden sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, damit weniger Meldungen, die eine entsprechend hohe Priorität haben, an das DMI-Terminal gesendet werden. Wenn der Schieberegler sich ganz rechts befindet, werden nur Meldungen des Typs „Kritisch“ an das DMI-Terminal gesendet.

   Ziehen Sie den Schieberegler nach links, damit mehr Alarmmeldungen gesendet werden, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, werden sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ gesendet.

   Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern und zum Dialogfeld Warnungs-Manager-Eigenschaften zurückzukehren.

6. Klicken Sie auf **Testen**, um eine Testmeldung an die DMI-Software zu senden. Wenn die Meldung nicht beim Empfänger ankommt:

   - Überprüfen Sie die Punkte, die im Hinweis auf Seite 150 aufgeführt sind.
   - Suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige nach einer Fehlermeldung.

7. Klicken Sie auf **OK**, um zur Seite DMI zurückzukehren.

8. Wenn Sie die Konfigurationsoptionen speichern und das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, klicken Sie auf **OK**. Wenn Sie die Änderungen speichern und das Konfigurieren von Warnungs-Manager fortsetzen möchten, klicken Sie auf **Übernehmen** und dann auf eine andere Registerkarte. Wenn Sie das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen.** Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Starten eines Programms, um eine Alarmmeldung zu senden

Warnungs-Manager kann Sie warnen, sobald ein Virus gefunden wurde, indem im Netzwerk ein Programm gestartet oder eine Stapelverarbeitungsdatei ausgeführt wird. Wenn in Ihrem Unternehmen z.B. mit Lotus cc:Mail oder einem speziellen E-Mail-Paket gearbeitet wird, können Sie eine Stapelverarbeitungsdatei schreiben, die Alarmmeldungen für die weitere Verteilung an das E-Mail-Paket sendet.

ANMERKUNG: Jedes Programm, das Warnungs-Manager startet, wird im Hintergrund, ohne sichtbare Benutzeroberfläche, ausgeführt.

Um ein Programm auszuführen, sobald der Scanner ein Virus gefunden hat, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.
2. Klicken Sie auf die Registerkarte Programm. Die Registerkarte Programm (siehe Abbildung 8-24) wird angezeigt.

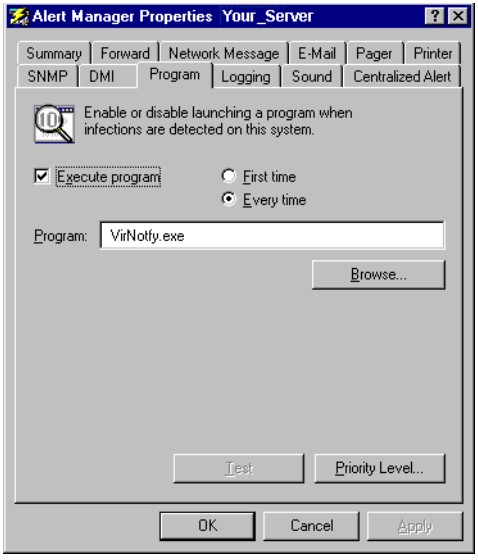


Abbildung 8-24. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „Programm“

3. Geben Sie den Namen und den Pfad des Programms ein, das Sie ausführen möchten, wenn der Scanner ein Virus gefunden hat, oder klicken Sie auf **Durchsuchen**, um die Programmdatei im Netzwerk zu suchen.

Warnungs-Manager führt standardmäßig das Programm VIRNOTFY.EXE aus, das ohne Oberfläche ausgeführt wird und Eingaben nur über zwei Variablen vom Scanner entgegennimmt, und zwar:

- %INFFILENAME% - Diese Variable gibt den Pfad und den Namen der infizierten Datei an.
- %VIRUSNAME% - Diese Variable gibt das infizierende Virus an.

Das Programm zeigt dann die Informationen, die das Virenschutzprogramm geliefert hat, in einem Dialogfeld zur Virusbenachrichtigung an, das auf dem Serverbildschirm angezeigt wird. Damit Sie weiterarbeiten können, müssen Sie auf **OK** klicken, um dieses Dialogfeld zu schließen.

❑ **ANMERKUNG:** Wenn Sie eine andere Anzeige für Virusbenachrichtigungen bevorzugen, können Sie eine eigene Anwendung oder Stapelverarbeitungsdatei schreiben, die diese Variablen auswertet.

---

4. Wenn Sie möchten, daß das Programm nur gestartet wird, wenn es das erste Mal ein Virus gefunden hat, aktivieren Sie die Option Erstes Mal. Soll das Programm jedesmal gestartet werden, wenn es ein Virus gefunden hat, aktivieren Sie die Option Jedesmal. Wenn Sie Erstes Mal ausgewählt haben, startet das von Ihnen angegebene Programm, wenn ein Virus zum ersten Mal auftritt. Wenn dieses Virus beim Scannen desselben Verzeichnisses nochmals auftritt, wird das Programm nicht mehr gestartet.

   Wenn Warnungs-Manager jedoch ein Virus findet, dann beim weiteren Scannen ein anderes Virus findet und anschließend eine weitere Kopie des ersten Virus gefunden wird, wird dasselbe Programm dreimal hintereinander gestartet. Wenn mehrere Instanzen desselben Programms gestartet werden, geht Ihrem Server möglicherweise der Speicher aus.

5. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmereignissen einen Programmstart auslösen sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, wenn Sie möchten, daß das Programm bei weniger Meldungen, die dafür eine entsprechend höhere Priorität haben, gestartet wird. Wenn der Schieberegler sich ganz rechts befindet, wird das Programm nur bei Meldungen des Typs „Kritisch“ gestartet.

Ziehen Sie den Schieberegler nach links, damit mehr Alarmmeldungen gesendet werden, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, werden sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ gesendet.

Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

6. Klicken Sie auf **Testen**, um festzustellen, ob die Software die Programme startet. Wenn das Programm nicht startet:

   - Überprüfen Sie die Punkte, die im Hinweis auf Seite 150 aufgeführt sind.
   - Suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige nach einer Fehlermeldung.

7. Klicken Sie auf **OK**, um die Änderungen zu speichern und zur Seite Programm zurückzukehren.

8. Wenn Sie die Konfigurationsoptionen speichern und das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, klicken Sie auf **OK**. Wenn Sie die Änderungen speichern und das Konfigurieren von Warnungs-Manager fortsetzen möchten, klicken Sie auf **Übernehmen** und dann auf eine andere Registerkarte. Wenn Sie das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**. Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Senden von Alarmmeldungen an Windows NT- oder Windows 2000-Systemprotokolle

Warnungs-Manager kann Alarmmeldungen, die der Scanner erstellt hat, an das Systemprotokoll auf jedem Server senden, der unter Windows NT 4.0 oder Windows 2000 läuft. Warnungs-Manager darf nicht unter einem Systemkonto, sondern muß unter einem benannten Konto ausgeführt werden, damit diese Warnmethode funktioniert Damit Alarmmeldungen, die mit dieser Methode gesendet werden, angezeigt werden, müssen Sie die Windows-Ereignisanzeige öffnen. Einzelheiten finden Sie in Ihrer Windows-Dokumentation.

Um Alarmmeldungen an ein Windows NT- oder Windows 2000-Systemprotokoll zu senden, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.

2. Klicken Sie auf die Registerkarte Protokollierung.

   Es wird die Seite Protokollierung (Abbildung 8-25 auf Seite 173) mit einer Liste aller Computer angezeigt, die Sie so eingerichtet haben, daß sie Alarmmeldungen empfangen. Wenn Sie noch keinen Computer so eingerichtet haben, daß er Alarmmeldungen empfängt, ist diese Liste leer.

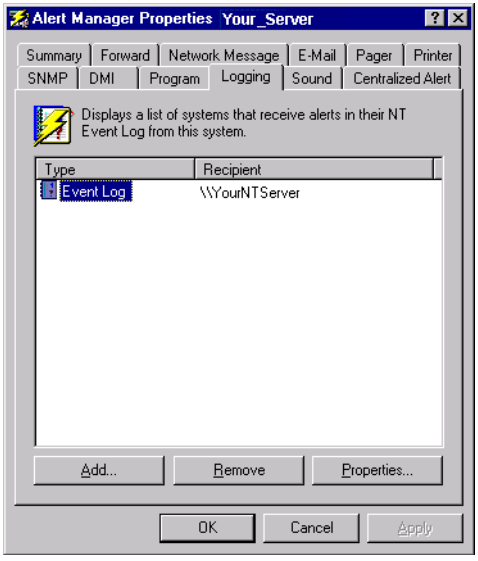


Abbildung 8-25. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „Protokollierung“

3. Sie können diese Liste wie folgt aktualisieren:

   - **Einen Computer aus der Liste entfernen.** Wählen Sie einen der aufgelisteten Computer aus, und klicken Sie dann auf **Entfernen.**
   - **Einen Computer zur Liste hinzufügen.** Klicken Sie auf **Hinzufügen**, um das Dialogfeld Protokollierungseigenschaften (siehe Abbildung 8-26 auf Seite 174) anzuzeigen. Geben Sie dann in das Textfeld den Namen des Zielcomputers ein, oder klicken Sie auf **Durchsuchen**, um den Computer im Netzwerk zu suchen. Fahren Sie danach mit Schritt 4 auf Seite 174 fort.

- **Konfigurationsoptionen ändern.** Wählen Sie einen der aufgelisteten Computer aus, und klicken Sie dann auf **Eigenschaften.** Das Dialogfeld Protokollierungseigenschaften wird angezeigt (siehe Abbildung 8-26 auf Seite 174). Ändern Sie im Textfeld **Drucker** die Informationen, die Sie ändern möchten. Fahren Sie danach mit Schritt 4 auf Seite 174 fort.

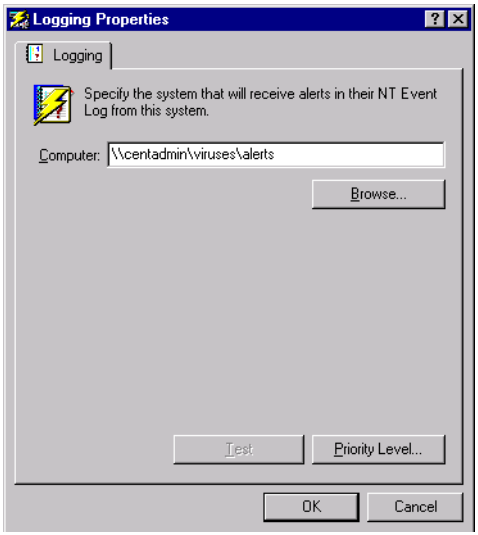


Abbildung 8-26. Dialogfeld „Protokollierungseigenschaften“

4. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmmeldungen in der Windows NT- oder Windows 2000-Ereignisanzeige protokolliert werden sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, damit weniger Meldungen, die eine entsprechend hohe Priorität haben, in der Windows-Ereignisanzeige protokolliert werden. Wenn der Schieberegler sich ganz rechts befindet, werden nur Meldungen des Typs „Kritisch“ in der Windows-Ereignisanzeige protokolliert.

   Ziehen Sie den Schieberegler nach links, damit mehr Alarmmeldungen gesendet werden, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, werden sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ gesendet.

   Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

5. Klicken Sie auf **Testen**, um eine Testmeldung an den Zielcomputer zu senden. Die Meldung wird im Systemprotokoll des Zielservers festgehalten. Öffnen Sie die Windows NT- oder Windows 2000-Ereignisanzeige, um die Meldung anzuzeigen. Wenn die Meldung nicht in der Ereignisanzeige erscheint:

   - Überprüfen Sie die Punkte, die im Hinweis auf Seite 150 aufgeführt sind.
   - Suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige des lokalen Computers nach einer Fehlermeldung.

6. Klicken Sie auf **OK**, um die Änderungen zu speichern und zur Seite Protokollierung zurückzukehren.

7. Wenn Sie die Konfigurationsoptionen speichern und das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, klicken Sie auf **OK**. Wenn Sie die Änderungen speichern und das Konfigurieren von Warnungs-Manager fortsetzen möchten, klicken Sie auf **Übernehmen** und dann auf eine andere Registerkarte. Wenn Sie das Dialogfeld Warnungs-Manager-Eigenschaften schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**. Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Abgeben einer Alarmmeldung durch Abspielen eines Tons

Warnungs-Manager kann, wenn ein Virus entdeckt wurde, einen Ton abspielen, um Sie zu warnen. Sie können einen Ton angeben, der als .WAV-Datei formatiert ist, oder Sie können Warnungs-Manager veranlassen, einen Standardwarnton abzuspielen.

Damit Warnungs-Manager einen Ton abspielt, sobald der Scanner ein Virus gefunden hat, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.

2. Klicken Sie auf die Registerkarte Ton.

   Die Registerkarte Ton (siehe Abbildung 8-27) wird angezeigt.

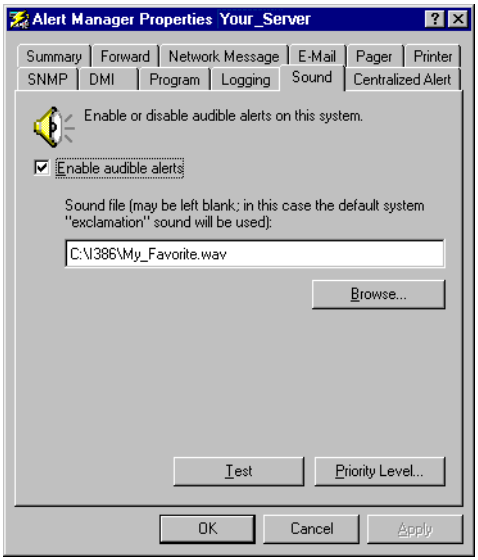


Abbildung 8-27. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „Ton“

3. Aktivieren Sie das Kontrollkästchen **Akustische Warnungen aktivieren**.

4. Geben Sie den Namen und den Pfad der Klangdatei ein, die die Virenschutzsoftware ausführen soll, wenn sie ein Virus gefunden hat, oder klicken Sie auf **Durchsuchen**, um die Klangdatei auf der Festplatte zu suchen.

   Standardmäßig spielt Warnungs-Manager den Ton aus der Datei WARNING.WAV ab, die sich im Installationsverzeichnis des Virenschutzprogramms befindet.

5. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmereignissen eine akustische Warnung auslösen sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, wenn Sie möchten, daß der Ton bei weniger Meldungen, die dafür eine entsprechend höhere Priorität haben, abgespielt wird. Wenn der Schieberegler sich ganz rechts befindet, wird nur bei Meldungen des Typs „Kritisch“ eine akustische Warnung ausgelöst.

Ziehen Sie den Schieberegler nach links, wenn mehr Alarmmeldungen das Abspielen eines Tons auslösen sollen, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, lösen sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ das Abspielen eines Tons aus.

Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

6. Klicken Sie auf **Testen**, um festzustellen, ob ein Ton abgespielt wird. Wenn Sie keinen Ton hören:

   - überprüfen Sie die Punkte, die im Hinweis auf Seite 150 aufgeführt sind.
   - suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige nach einer Fehlermeldung.

7. Klicken Sie auf **OK**, um die Änderungen zu speichern und zur Seite **Ton** zurückzukehren.

8. Um andere Benachrichtigungsoptionen zu konfigurieren, klicken Sie auf eine andere Registerkarte. Wenn Sie die Änderungen speichern möchten, ohne das Dialogfeld Warnungs-Manager-Eigenschaften zu schließen, klicken Sie auf **Übernehmen**. Wenn Sie die Änderungen speichern und das Dialogfeld schließen möchten, klicken Sie auf **OK**. Wenn Sie das Dialogfeld schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**. Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Senden einer Alarmmeldung an Terminal Server-Clients

Die Registerkarte Terminal Server wird nur angezeigt, wenn Warnungs-Manager und Terminal Server auf demselben Server installiert sind.

Um Alarmmeldungen an die Clientarbeitsstationen von Terminal Server zu senden, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.

2. Klicken Sie auf die Registerkarte Terminal Server. Die Registerkarte Terminal Server wird angezeigt (siehe Abbildung 8-28).

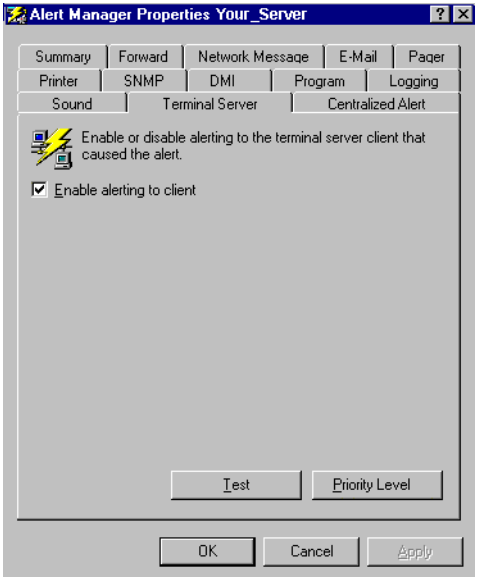


Abbildung 8-28. Dialogfeld „Warnungs-Manager-Eigenschaften“ - Seite „Terminal Server“

3. Aktivieren Sie **Warnung für Client aktivieren**. Warnungs-Manager sendet eine Meldung an die Arbeitsstation, an der der Benutzer eine Aktion ausgeführt hat, die zur Entdeckung eines Virus geführt hat.

TIP: Wenn Sie Terminal Server als Warnmethode verwenden, empfiehlt McAfee, daß Sie als Methode für das Senden von Meldungen keine Netzwerkmeldung verwenden. Die Methode Terminal Server sendet eine Alarmmeldung an den Computer, der die Alarmmeldung erstellt hat. Bei der Netzwerkmeldungsmethode wird eine Meldung an alle Terminal Server-Clients gesendet. Weitere Informationen über die Netzwerkmeldungsmethode finden Sie unter “Senden einer Alarmmeldung als Netzwerkmeldung“ auf Seite 151.

---

4. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Typen von Alarmereignissen eine Alarmmeldung auslösen sollen.

   Ziehen Sie im Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149) den Schieberegler nach rechts, wenn Sie möchten, daß der Ton bei weniger Meldungen, die dafür eine entsprechend höhere Priorität haben, abgespielt wird. Wenn der Schieberegler sich ganz rechts befindet, wird nur bei Meldungen des Typs „Kritisch“ eine akustische Warnung ausgelöst.

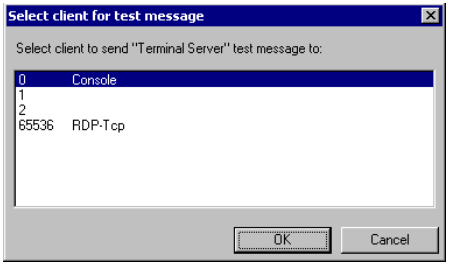
Ziehen Sie den Schieberegler nach links, wenn mehr Alarmmeldungen das Abspielen eines Tons auslösen sollen, also auch Alarmmeldungen mit einer niedrigeren Priorität. Wenn sich der Schieberegler ganz links befindet, lösen sowohl Meldungen der Typen „Information“ und „Warnung“ als auch solche der Typen „Gering“, „Schwer“ und „Kritisch“ das Abspielen eines Tons aus.

Informationen, wie die Prioritätsstufen für unterschiedliche Meldungstypen eingestellt werden, finden Sie unter “Anpassen von Alarmmeldungen“ auf Seite 182.

5. Klicken Sie auf **Übernehmen**, wenn die Änderungen gespeichert werden sollen, ohne daß das Dialogfeld geschlosen wird. Sie können diese Warnmethode jetzt testen, um sich zu vergewissern, daß sie wie erwartet funktioniert.

6. Klicken Sie auf **Testen**, um eine Testmeldung an eine Clientarbeitsstation zu senden. Es wird das Dialogfeld Client für Testmeldung auswählen angezeigt (siehe Abbildung 8-29).

Dialogfeld bei Windows NT 4



Dialogfeld bei Windows 2000

Abbildung 8-29. Dialogfeld „Warnungs-Manager-Eigenschaften“ Terminal Server-Dialogfeld zum Auswählen eines Clients

7. Verwenden Sie , um die Arbeitsstation auszuwählen, an die die Alarmmeldung gesendet werden soll. Wenn die Meldung nicht beim Client ankommt:

   - überprüfen Sie die Punkte, die im Hinweis auf Seite 150 aufgeführt sind.
   - suchen Sie in der Windows NT- oder Windows 2000-Ereignisanzeige nach einer Fehlermeldung.

8. Klicken Sie auf **OK**, um die Änderungen zu speichern und zur Seite **Ton** zurückzukehren.

9. Um andere Benachrichtigungsoptionen zu konfigurieren, klicken Sie auf eine andere Registerkarte. Wenn Sie die Änderungen speichern möchten, ohne das Dialogfeld Warnungs-Manager-Eigenschaften zu schließen, klicken Sie auf **Übernehmen**. Wenn Sie die Änderungen speichern und das Dialogfeld schließen möchten, klicken Sie auf **OK**. Wenn Sie das Dialogfeld schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

> **ANMERKUNG:** Ein Klicken auf **Abbrechen** bewirkt nicht, daß die Änderungen rückgängig gemacht werden, die Sie bereits durch Klicken auf **Übernehmen** gespeichert haben.

Einrichten der zentralen Warnung

Mit zentralen Warnungen wird der Warnungs-Manager in die Lage versetzt, Sie immer dann zu benachrichtigen, wenn auf irgendeiner Arbeitsstation des Netzwerks, auf der ein McAfee-Virenschutz-Clientprodukt, wie z.B. das Virenschutzprogramm McAfee VirusScan, installiert und korrekt konfiguriert ist, ein Virus entdeckt wurde. Alarmmeldungen, die von anderen McAfee-Virenschutzprogrammen für Clients gesendet wurden, werden bei einer zentralen Warnung an den dafür vorgesehenen Ordner auf dem Server weitergeleitet. Damit Sie diese Methode nutzen können, müssen Sie die Clientsoftware so konfigurieren, daß sie Alarmmeldungen an den Alarmordner sendet, und müssen Sie Warnungs-Manager anweisen, den Ordner auf Aktivitäten zu überwachen. Sobald die Methode für eine zentrale Warnung aktiviert wurde, versetzt sie Warnungs-Manager in die Lage, jede Alarmmeldung, die im Alarmordner gefunden wird, abzurufen und mit den Warnmethoden zu verteilen, die Sie konfiguriert haben.

Um die zentrale Warnung zu aktivieren, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Eigenschaften. Weitere Informationen erhalten Sie unter “Öffnen der Registerkarten von Warnungs-Manager“ auf Seite 144.
2. Klicken Sie auf die Registerkarte Zentrale Warnung. Die Registerkarte Zentrale Warnung wird angezeigt (siehe Abbildung 8-30).

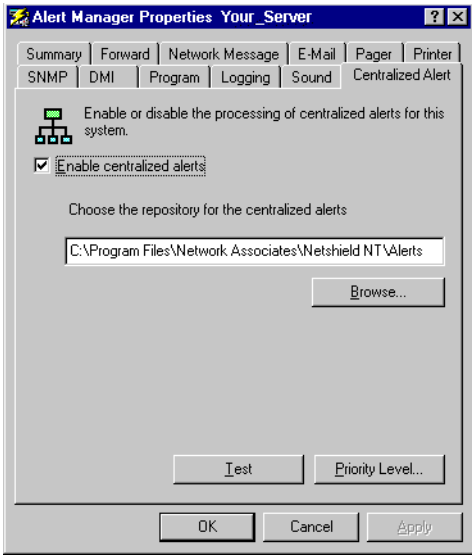


Abbildung 8-30. Registerkarte „Zentrale Warnung“

3. Aktivieren Sie **Zentrale Warnungen aktivieren.** Warnungs-Manager ist standardmäßig so konfiguriert, daß dieses Kontrollkästchen aktiviert ist.

4. Erstellen Sie auf dem Server einen Ordner mit einem aussagefähigen Namen, wie z.B. Alarm. Wenn die Clientsoftware ein Virus entdeckt hat, sendet sie eine Alarmmeldung als Textdatei in diesen dafür vorgesehenen Alarmordner. Warnungs-Manager wandelt die jeweilige Textmeldung in sein eigenes Format um und verteilt die Meldung über die Methoden, die Sie konfiguriert haben. Sobald die Textdatei verteilt wurde, wird sie aus dem Alarmordner gelöscht.

5. Geben Sie den Pfad des Alarmordners in das vorgesehene Textfeld ein. Sie können auf **Durchsuchen** klicken, um den Ordner auszuwählen.

   Wenn Sie Warnungs-Manager als Ressource in einem Cluster verwenden, muß sich der Ordner, in dem die Alarmmeldungen gesammelt werden, auf dem freigegebenen Datenträger des Clusters befinden.

   Damit Arbeitsstationen des Netzwerks Meldungen an diesen Ordner senden können, müssen alle Benutzer folgende Rechte für diesen Ordner haben: Erstellen, Schreiben und Löschen. Einzelheiten finden Sie in Ihrer Windows-Dokumentation.

6. Klicken Sie auf **OK**, um das Dialogfeld Warnungs-Manager-Eigenschaften zu schließen.

7. Konfigurieren Sie jede Arbeitsstation, auf der McAfee-Virenschutzsoftware für Clients ausgeführt wird, so, daß sie Alarmmeldungen an den Alarmordner sendet, den Sie festgelegt haben.

   Normalerweise ist dazu nur erforderlich, daß Sie in der Clientsoftware die zentrale Warnung aktivieren und den korrekten Alarmordner auf dem Server zuweisen. Ausführliche Informationen finden Sie im Handbuch des jeweiligen Clientpaketes, mit dem Sie arbeiten.

   ❑ **ANMERKUNG:** Damit die Clientsoftware einen Ordner als den korrekten Ordner für zentrale Warnungen erkennt, muß der Ordner eine Kopie der Datei CENTALRT.TXT enthalten. Wenn Sie der Clientsoftware einen Ordner angeben, der diese Textdatei nicht enthält, werden Alarmmeldungen von den Clients nicht korrekt gesendet.

   Die Virenschutzsoftware übergibt die Informationen aus der Textdatei dann an Warnungs-Manager, der die Datei mit allen Methoden verteilt, die Sie für den Einsatz konfiguriert haben. Das Virenschutzprogramm löscht die Textdatei anschließend aus dem Alarmordner.

Anpassen von Alarmmeldungen

Warnungs-Manager wird mit vielen Meldungen geliefert, die die jeweilige Situation beschreiben, in der die Software ein Virus entdeckt hat. Jede Alarmmeldung hat eine voreingestellte Prioritätsstufe und enthält Variablen, die die infizierte Datei und das infizierte System angeben, den infizierenden Virus benennen und weitere Informationen bereitstellen, die Sie in die Lage versetzen, einen schnellen und umfassenden Überblick über die Situation zu bekommen.

Sie können aber einzelne Alarmmeldungen aktivieren oder deaktivieren oder den Inhalt und die Prioritätsstufe einer Meldung ändern, um diese an Ihre Gegebenheiten anzupassen. Allerdings sollten Sie den Grundtenor jeder Alarmmeldung, die Sie bearbeiten, beibehalten.

Um das Dialogfeld Warnungs-Manager-Meldungen anzuzeigen, zeigen Sie im Menü **Start** auf **Programme**. Zeigen Sie dann auf das Untermenü **Network Associates**, und wählen Sie den Befehl Warnungs-Manager-Meldungen konfigurieren. Das Dialogfeld Warnungs-Manager-Meldungen wird angezeigt (siehe Abbildung 8-31).

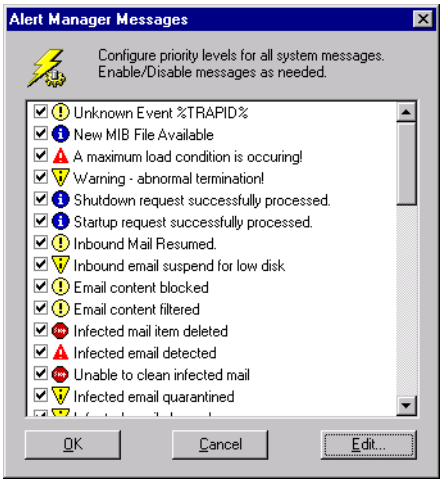


Abbildung 8-31. Dialogfeld „Warnungs-Manager-Meldungen“

ANMERKUNG: Von GroupShield für Exchange werden nur solche Alarmmeldungen verwendet, die mit GroupShield für Exchange beginnen.

Aktivieren und Deaktivieren von Alarmmeldungen

Warnungs-Manager kann Sie immer dann warnen, wenn der Scanner ein Virus gefunden oder wenn sich irgendein Aspekt des normalen Betriebs von Warnungs-Manager erheblich geändert hat. Möglicherweise möchten Sie jedoch nicht unter allen diesen Umständen Alarmmeldungen empfangen. Warnungs-Manager ist standardmäßig so konfiguriert, daß seine sämtlichen Alarmmeldungen aktiviert sind. Wenn Sie für bestimmte Alarmmeldungen verhindern möchten, daß sie von Warnungs-Manager gesendet werden, verwenden Sie das Dialogfeld Warnungs-Manager-Meldungen, um die unerwünschten Meldungen zu deaktivieren.

Um Alarmmeldungen zu aktivieren oder zu deaktivieren, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Meldungen.
2. Überprüfen Sie die Liste der angezeigten Meldungen. Um eine Meldung zu deaktivieren, die Warnungs-Manager nicht senden soll, deaktivieren Sie das Kontrollkästchen links neben der Meldung. Lassen Sie das Kontrollkästchen neben jeder Meldung, die Warnungs-Manager senden *soll*, aktiviert.

3. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld Warnungs-Manager-Meldungen zu schließen. Wenn Sie das Dialogfeld schließen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Ändern der Priorität einer Alarmmeldung

Einige Situationen, die der Scanner vorfindet, erfordern eine unmittelbarere Aufmerksamkeit als andere. Die Prioritätsstufe jeder Alarmmeldung ist auf einen Standardwert eingestellt, der der Dringlichkeit entspricht, die die meisten Systemadministratoren der Meldung zuweisen würden. Sie können die Werte dieser Prioritätsstufen ändern, um sie an Ihre eigenen Anforderungen anzupassen, und Sie können diese Werte verwenden, um die Meldungen zu filtern, die Sie von Warnungs-Manager empfangen haben, so daß Sie sich zunächst auf die wichtigsten Meldungen konzentrieren können.

Um die Prioritätsstufe zu ändern, die einer Alarmmeldung zugeordnet ist, führen Sie folgende Schritte aus:

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften, und klicken Sie auf die Registerkarte Warnungen.
2. Klicken Sie im Feld Warnungs-Manager auf **Warnungen bearbeiten**, um das Dialogfeld **Warnungs-Manager-Meldungen** anzuzeigen.
3. Wählen Sie eine der aufgelisteten Alarmmeldungen von GroupShield für Exchange aus, und klicken Sie dann auf **Bearbeiten.**

> **ANMERKUNG:** Die anderen Alarmmeldungen, die im Dialogfeld aufgelistet sind, wurden vom Dienstprogramm Warnungs-Manager installiert, werden aber nicht von GroupShield für Exchange verwendet.

Das Dialogfeld Warnungs-Manager-Meldung bearbeiten wird angezeigt (siehe Abbildung 8-32).

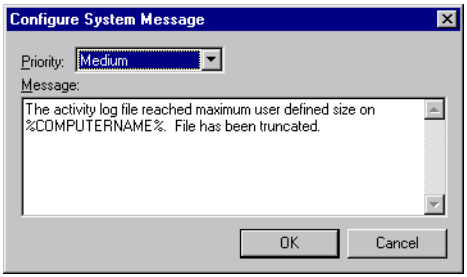


Abbildung 8-32. Dialogfeld „Systemmeldung konfigurieren“

4. Wählen Sie in der Liste Priorität eine Prioritätsstufe aus. Sie können jeder Meldung eine der folgenden Prioritätsstufen zuweisen: **Information**, **Warnung**, **Gering**, **Schwer** oder **Kritisch**.

   Das Symbol neben jeder Meldung zeigt Ihnen an, welche Prioritätsstufe der Meldung momentan zugewiesen ist:

   Kennzeichnet eine Meldung des Typs „Information“.

   Kennzeichnet eine Meldung des Typs „Warnung“.

   Kennzeichnet eine Meldung, die eine relativ geringe Wichtigkeit hat.

   Kennzeichnet eine Meldung, die eine höhere Wichtigkeit hat.

   Kennzeichnet eine Meldung, die eine kritische Wichtigkeit hat.

   Wenn Sie einer Meldung eine andere Priorität zuweisen, ändert sich das Symbol neben der Meldung, um den neuen Prioritätsstaus zu zeigen.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld Warnungs-Manager-Meldung bearbeiten zu schließen.

6. Wenn Sie nach Meldungen filtern möchten, konfigurieren Sie jede von Ihnen in Warnungs-Manager eingerichtete Warnmethode so, daß sie für die Weiterleitung nur Meldungen akzeptiert, die eine bestimmte Priorität haben.

   Nehmen Sie z.B. an, Sie möchten, daß Warnungs-Manager Sie immer dann informiert, wenn der Scanner einen Virus auf Ihrem Server gefunden hat, aber Sie möchten nicht, daß Warnungs-Manager Ihnen routinemäßige Betriebsmeldungen sendet. Statt dessen kann der Warnmanager die Routinemeldungen über E-Mail oder andere, weniger wichtige Methoden senden.

   Um dies zu erreichen, öffnen Sie über das Dialogfeld Warnungs-Manager-Meldungen das Dialogfeld Warnungs-Manager-Meldung bearbeiten, um Viruswarnungen eine hohe Priorität und Routinemeldungen eine mittlere oder niedrige Priorität zuzweisen (siehe Abbildung 8-31 auf Seite 183). Im nächsten Schritt müssen Sie Warnungs-Manager anweisen, nur Meldungen mit hoher Priorität an Ihren Pager zu senden.

Dazu kehren Sie zum Dialogfeld Warnungs-Manager-Eigenschaften (siehe Abbildung 8-8 auf Seite 146) zurück und klicken auf die Registerkarte für die Methode, die Sie ändern möchten. Wechseln Sie zu dem Abschnitt in diesem Kapitel weiter oben, in dem die Warnmethode beschrieben ist, die Sie ändern möchten, und lesen Sie die Anleitungen für das Dialogfeld Prioritätsstufe (siehe Abbildung 8-11 auf Seite 149).

Ändern des Textes einer Alarmmeldung

Damit Sie besser auf eine Situation reagieren können, die Ihre Aufmerksamkeit erfordert, enthält das Dienstprogramm Warnungs-Manager zum einen genügend Informationen in seinen Alarmmeldungen, um die Ursache jedes aufgetretenen Problems zu benennen, und zum anderen einige Informationen über die Umstände, unter denen das Problem aufgetreten ist. Sie können Informationen oder Kommentare zu einer Alarmmeldung hinzufügen, die das jeweilige Problem eingehender erläutern, Leute auflisten, die bei der Behebung behilflich sein können, oder den Empfänger dabei unterstützen, die zu unternehmenden Schritte zu verstehen.

WICHTIG: Sie können zwar den Text jeder Alarmmeldung bearbeiten, damit er den von Ihnen gewünschten Inhalt hat, Sie sollten aber versuchen, die wesentliche Aussage beizubehalten, da Warnungs-Manager die jeweilige Meldung nur sendet, wenn der Scanner bestimmte Bedingungen vorfindet. Zum Beispiel sendet Warnungs-Manager die Alarmmeldung „Task wurde gestartet“ nur, wenn der Scanner tatsächlich einen Task startet.

Um den Text einer Alarmmeldung anzupassen, führen Sie folgende Schritte aus:

1. Öffnen Sie das Dialogfeld Warnungs-Manager-Meldungen.
2. Wählen Sie eine der Alarmmeldungen aus, und klicken Sie dann auf **Bearbeiten.**

   Das Dialogfeld Warnungs-Manager-Meldung bearbeiten wird angezeigt (siehe Abbildung 8-32 auf Seite 184).
3. Ändern oder ergänzen Sie den angezeigten Text. Text, der in Prozentzeichen eingeschlossen ist, z.B. %COMPUTERNAME%, gibt den Namen einer Variablen an, die das Programm durch einen tatsächlichen Wert ersetzt, bevor Warnungs-Manager die Alarmmeldung erstellt.

Die Variablen sind in der folgenden Tabelle mit einer Beschreibung des zugehörigen Wertes aufgelistet, dem sie jeweils entsprechen:

Variablenname	Ersetzt durch tatsächlichen Wert
%COMPUTERNAME%	Der Name eines Computers, wie er im Netzwerk angezeigt wird. Dies kann ein infizierter Computer, ein Computer, der einen Gerätetreiberfehler gemeldet hat, oder irgendein anderer Computer sein, mit dem der Scanner verbunden ist.
%DATE%	Das Datum, an dem ein Scanvorgang ein Virus entdeckt hat.
%DATVERSION%	Die Version der Virusdefinitionsdateien, die der Scanner verwendet hat, als er ein Virus entdeckte.
%ENGINEVERSION%	Die Version der Scan-Engine, die verwendet wurde, als der Scanner ein Virus entdeckt hat.
%FILENAME%	Der Name einer Datei, die infiziert ist oder bei der der Scanner versucht hat, sie aus einem Scanvorgang auszuschließen.
%SOFTWARENAME%	Der Name einer ausführbaren Datei, bei der ein Virus entdeckt wurde, von der ein Fehler übermittelt wurde oder bei der der Scanner zum Einsatz kam.
%SOFTWAREVERSION%	Die Versionsnummer eines aktiven Softwarepaketes, bei dem ein Virus entdeckt wurde, von dem ein Fehler übermittelt wurde oder bei dem der Scanner zum Einsatz kam.

Variablenname	Ersetzt durch tatsächlichen Wert
%SOURCEIP%	Die IP-Adresse eines Computers. Dies kann ein infizierter Computer, ein Computer, der einen Gerätetreiberfehler gemeldet hat, oder irgendein anderer Computer sein, mit dem der Scanner verbunden ist.
%TASKNAME%	Der Name eines aktiven Tasks, wie z.B. desjenigen, bei dem ein Virus entdeckt wurde, von dem ein Fehler übermittelt wurde oder bei dem der Scanner zum Einsatz kam.
%TIME%	Die Uhrzeit, zu der der Scanner eine Scanaktivität ausführte.
%USERNAME%	Der Name des Benutzers, der momentan am Server angemeldet ist. Dies kann Ihnen z.B. mitteilen, ob jemand einen Scanvorgang abgebrochen hat.
%VIRUSNAME%	Der Name eines infizierenden Virus.

4. Klicken Sie auf **OK**, um die Änderungen zu speichern und zum Dialogfeld Warnungs-Manager-Meldungen zurückzukehren. Klicken Sie dann erneut auf **OK**, um zur Serververwaltungskonsole GroupShield-Eigenschaften zurückzukehren.

Protokollier- und Überwachungsfunktionen 9

GroupShield für Exchange bietet zwei Hauptmethoden zum Protokollieren und Überwachen von Systemereignissen und Virenschutzaktivitäten auf einem Microsoft Exchange-Server:

- McAfee Log Manager
- Systemmonitor von GroupShield für Exchange

Einführung in McAfee Log Manager

McAfee Log Manager versorgt Administratoren mit nützlichen Informationen über Systemereignisse und Virusinfektionen in einem Format, das einfach zu verwenden und zu lesen ist. Log Manager besteht aus drei verschiedenen Bereichen zur Konfiguration und Informationsanzeige:

- Die Optionen, die über “McAfee Log Manager” verfügbar sind, sind auf Seite 190 beschrieben
- Die Optionen, die über “Die Symbolleiste” verfügbar sind, sind auf Seite 192 beschrieben
- Die Inhalte des “Das Ergebnisfenster” sind auf Seite 193 beschrieben

Unter “Konfigurieren der McAfee Log Manager-Ausgabe“ auf Seite 125 erfahren Sie, wie das McAfee-Dienstprogramm Log Manager geöffnet wird.

Die Benutzeroberfläche

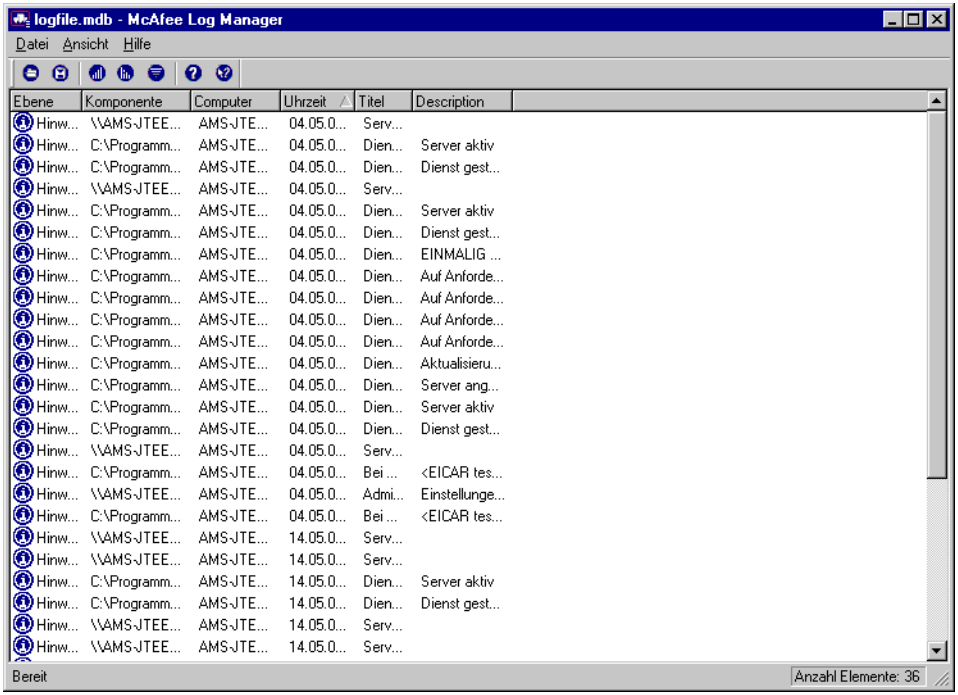


Abbildung 9-1. McAfee Log Manager

Die Menüleiste

Verwenden Sie die Menüleiste, um McAfee Log Manager zu konfigurieren und Informationen über die einzelnen aufgezeichneten Ereignisse anzuzeigen.

Das Menü „Datei“

- Der Befehl **Öffnen** öffnet eine zuvor gespeicherte Log Manager-Datenbank oder eine Datenbank, die auf einem anderen Server abgelegt worden ist.

  Verwenden Sie den Befehl Speichern unter oder in der Symbolleiste, um eine Log Manager-Datenbank zu speichern.

ANMERKUNG: Verwenden Sie die Netzwerkumgebung, um Log Manager auf einem anderen Server zu starten. Möglicherweise benötigen Sie dazu einen Benutzernamen und ein Kennwort.

- Der Befehl **Speichern unter** legt die aktuelle Ansicht von Log Manager zu Analyse- oder Archivierungszwecken unter einem anderen Dateinamen ab.

ANMERKUNG: Der Befehl Speichern unter dient dazu, eine „Momentaufnahme“ der Datenbank zu speichern, um sie beispielsweise an den Support von Network Associates zu senden. Die im .CSV-Format gespeicherte Log Manager-Datei läßt sich nach Microsoft Excel importieren, wo sie analysiert und ausgewertet werden kann.

Um eine gespeicherte Ansicht von McAfee Log Manager anzuzeigen, verwenden Sie den Befehl **Öffnen** im Menü **Datei**.

- Mit dem Befehl **Gefilterte Datensätze löschen** werden gefilterte Datensätze aus der Log Manager-Datenbank entfernt.

  Auch dieser Vorgang kann nicht rückgängig gemacht werden.

- Mit dem Befehl **Gesamtes Protokoll löschen** werden alle Datensätze aus der Log Manager-Datenbank entfernt.

  Auch dieser Vorgang kann nicht rückgängig gemacht werden.

- **Beenden** schließt das Log Manager-Programm.

Das Menü "Ansicht"

- Der Befehl **Aktualisieren** fügt Datensätze hinzu, die seit dem Laden der Log Manager-Datenbank neu protokolliert worden sind.
- Der Befehl **Filter** erstellt, ändert und löscht Protokollfilter. Informationen, wie Objekte im Ergebnisfenster gefiltert werden können, finden Sie unter “Filtern von Protokolldatensätzen“ auf Seite 196.
- Der Befehl **Spalten** dient der Festlegung, welche der Spalten im Ergebnisfenster sichtbar sein sollen.

ANMERKUNG: Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, um die zugehörigen Konfigurationsoptionen anzuzeigen.

- Der Befehl **Details** zeigt eine Übersicht aller Informationen über einen Datensatz an.

ANMERKUNG: Um eine Aufstellung von Detailinformationen (zu einem Datensatz) anzuzeigen, markieren Sie in der Spalte Grad den Datensatz und wählen dann im Menü Ansicht den Befehl **Details**. Die Spalte **Grad** muß dabei im Ergebnisfenster sichtbar sein. Zur Festlegung der sichtbaren Spalten verwenden Sie die Option **Spalten**.

Der untere Teil des Menüs **Ansicht** enthält Optionen für die einzelnen Log Manager-Komponenten. Klicken Sie auf einen Eintrag, um bestimmte Komponenten innerhalb der Ansicht ein- oder auszublenden.

Das Menü „Hilfe“

Im Menü Hilfe können Sie die folgenden Optionen wählen:

- Der Befehl **Hilfethemen** öffnet diese Hilfedatei von McAfee Log Manager.
- Der Befehl **Info** öffnet ein Dialogfeld mit Copyright-Informationen zu Log Manager und Systeminformationen über den aktuellen Microsoft Exchange-Server. Das Dialogfeld ermöglicht außerdem eine Verbindung mit der Network Associates-Website für den technischen Support.

  Klicken Sie im Dialogfeld Info auf **OK**, um zu Log Manager zurückzukehren.

Die Symbolleiste

Verwenden Sie die Symbolleiste, um die Ansicht für Log Manager festzulegen, Copyright-Informationen anzuzeigen und Hilfe zu erhalten. Folgende Optionen sind verfügbar:

Öffnet eine zuvor gespeicherte Log Manager-Datenbank oder eine Datenbank, die auf einem anderen Server abgelegt worden ist.

Verwenden Sie den Befehl Speichern unter oder in der Symbolleiste, um eine Log Manager-Datenbank unter einem anderen Namen zu speichern.

ANMERKUNG: Verwenden Sie die Netzwerkumgebung, um Log Manager auf einem anderen Server zu starten. Möglicherweise benötigen Sie dazu einen Benutzernamen und ein Kennwort.

---

speichert die aktuelle Ansicht von Log Manager in einer anderen Datei.

ANMERKUNG: Der Befehl Speichern unter dient dazu, eine „Momentaufnahme“ der Datenbank zu speichern, um sie beispielsweise an den Support von Network Associates zu senden. Die im CSV-Format gespeicherte Log Manager-Datei läßt sich nach Microsoft Excel importieren, wo sie analysiert und ausgewertet werden kann. Um eine gespeicherte Protokolldatei anzuzeigen, verwenden Sie den Befehl **Öffnen** im Menü **Datei**.

---

sortiert die Datensätze derart, daß der kleinste Datensatz am oberen Ende des Ergebnisfensters erscheint.

sortiert die Datensätze derart, daß der größte Datensatz am oberen Ende des Ergebnisfensters erscheint.

öffnet das Dialogfeld Filterabfrage, in dem Sie Protokollfilter definieren, ändern oder löschen können. “Filtern von Protokolldatensätzen“ auf Seite 196 für Informationen, wie das Dialogfeld Filterabfrage verwendet werden kann.

öffnet das Fenster Info. Das Fenster zeigt die Copyright-Details zu Log Manager sowie Systeminformationen über den aktuellen Server an und ermöglicht eine Verbindung mit der Network Associates-Website für den technischen Support.

Klicken Sie im Dialogfeld Info auf **OK**, um zu Log Manager zurückzukehren.

startet die Direkthilfe. Klicken Sie auf dieses Symbol und anschließend auf ein Objekt auf dem Bildschirm, um kontextabhängige Hilfe zu erhalten.

Das Ergebnisfenster

Das Ergebnisfenster zeigt Informationen über protokollierte Ereignisse an. Das Fenster ist in sechs verschiedene Informationsspalten aufgeteilt:

- **Grad** zeigt die Wichtigkeit des protokollierten Ereignisses an.
- **Komponente** verweist auf das Systemobjekt, welches das Ereignis verursacht hat.
- **Computer** gibt den Computer an, auf dem das Ereignis stattfand.
- **Zeitpunkt** zeigt den Zeitpunkt an, zu dem das Ereignis stattfand.
- **Bezeichnung** gibt an, welches Systemereignis oder Virusereignis stattgefunden hat.
- **Beschreibung** bezeichnet die Aktion, die als Reaktion auf das Ereignis durchgeführt worden ist.

ANMERKUNG: Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, um die zugehörigen Konfigurationsoptionen anzuzeigen.

Ergänzende Informationen

- Ein in Rot hervorgehobener Spaltenname mit dem zusätzlichen Symbol zeigt an, daß diese Spalte einen aktiven Filter repräsentiert.
- zeigt an, daß die Spalte am oberen Ende des Ergebnisfensters den ältesten Datensatz enthält.
- zeigt an, daß die Spalte am oberen Ende des Ergebnisfensters den neuesten Datensatz enthält.
- Verwenden Sie das Menü Ansicht, um Typ und Darstellung der im Ergebnisfenster sichtbaren Informationen zu ändern. Informationen, wie die Befehle des Menüs Ansicht verwendet werden können, finden Sie unter “Das Menü "Ansicht"“ auf Seite 191.

Arbeiten mit Log Manager

Speichern der Protokolldatenbank

Sie können eine „Momentaufnahme“ der Datenbank in einer Datei ablegen, um sie beispielsweise an den Support von Network Associates zu senden oder zu archivieren.

Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie McAfee Log Manager, und wählen Sie eine der folgenden Möglichkeiten:

- Klicken Sie in der Symbolleiste auf .
- Wählen Sie im Menü **Datei** den Befehl **Speichern unter**.

2. Wechseln Sie im Dialogfeld Speichern unter (Abbildung 9-2) zu dem Ordner auf Ihrem Computer oder im Netzwerk, in dem die Datenbank abgelegt werden soll.

Abbildung 9-2. McAfee Log Manager - Dialogfeld „Speichern unter“

3. Geben Sie gegebenenfalls einen eindeutigen Dateinamen in das dafür vorgesehene Textfeld ein.

   McAfee empfiehlt, bei jeder Speicherung des Datenbankzustands jeweils einen anderen eindeutigen Dateinamen zu wählen, um eine spätere Identifizierung zu erleichtern.

4. Klicken Sie auf **Speichern**.

ANMERKUNG: Einer gespeicherten Kopie der Datenbank werden keine neuen Datensätze mehr hinzugefügt, nachdem der Speicherungsvorgang abgeschlossen ist.

Öffnen einer archivierten Protokolldatenbank

Die Protokolldatenbank kann zu Archivierungszwecken unter einem anderen Dateinamen auf Ihrem Computer oder im Netzwerk gespeichtert werden.

Um eine archivierte Datenbank zu öffnen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie Log Manager, und wählen Sie im Menü **Datei** den Befehl **Öffnen**.
2. Wechseln Sie im Dialogfeld Öffnen (Abbildung 9-3) zu dem Ordner auf Ihrem Computer oder im Netzwerk, in dem die archivierte Kopie der Datenbank gespeichert ist.

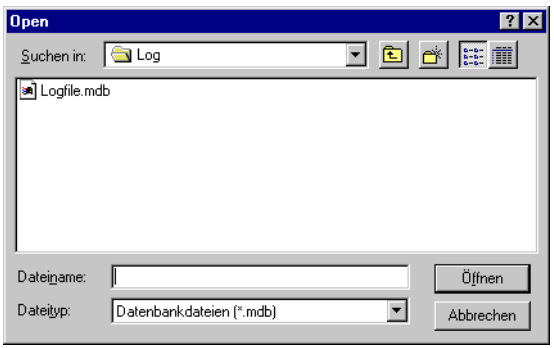


Abbildung 9-3. McAfee Log Manager - Dialogfeld „Öffnen“

3. Markieren Sie im Dialogfeld Öffnen den Namen der Datei, und klicken Sie dann auf **Öffnen**.

Abrufen von Datensatzdetails

Verwenden Sie das Fenster Datensatzdetails, um eine Zusammenfassung der Informationen über einen ausgewählten Datensatz zu erhalten. Zu diesen Informationen gehören der Name des Objekts oder Ereignisses, der Ort, an dem sich das Objekt auf dem Computer befindet, sowie alle Virenschutzaktionen, die durch GroupShield für Exchange vorgenommen wurden.

Zum Anzeigen von Informationen zu einem bestimmten Datensatz führen Sie die folgenden Schritte aus:

1. Öffnen Sie Log Manager. Wählen Sie in der Spalte Grad den Datensatz aus, den Sie anzeigen möchten.

2. Wählen Sie aus dem Menü **Ansicht** den Befehl **Details**, um das Dialogfeld Datensatzdetails (Abbildung 9-4) anzuzeigen.

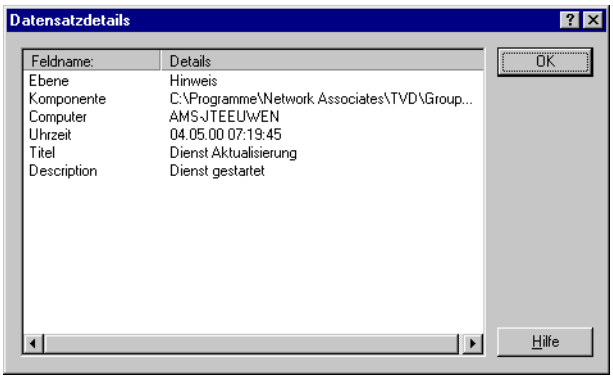


Abbildung 9-4. McAfee Log Manager - Dialogfeld „Datensatzdetails“

3. Klicken Sie auf **OK**, um zum Ergebnisfenster von Log Manager zurückzukehren.

Filtern von Protokolldatensätzen

Ein Filter organisiert die Menge der sichtbaren Datensätze im Ergebnisfenster in Form einer besser an die Informationsbedürfnisse angepaßten Menge, indem er Datensätze aus der Menge entfernt, die nicht mit den von Ihnen angegebenen Parametern übereinstimmen. Es können mehrere Filter auf eine Spalte angewendet werden, und es können mehrere Spalten gleichzeitig gefiltert werden.

Hinzufügen eines neuen Filters

Verwenden Sie das Dialogfeld Filterabfrage, um Filter für die Log Manager-Datenbank zu definieren, zu modifzieren und zu entfernen.

Um einen neuen Filter hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Log Manager-Datenbank, und wählen Sie eine der folgenden Optionen, um das Dialogfeld Filterabfrage (Abbildung 9-5 auf Seite 197) anzuzeigen:

- Klicken Sie in der Symbolleiste auf .
- Wählen Sie aus dem Menü **Ansicht** den Befehl **Filter**.

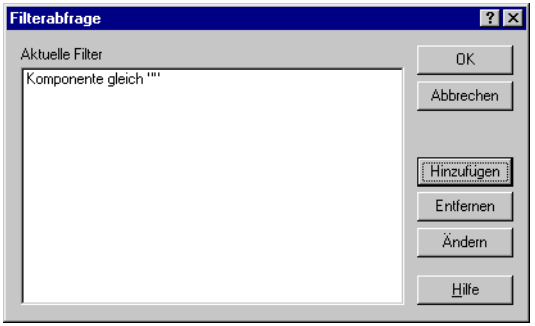


Abbildung 9-5. McAfee Log Manager - Dialogfeld „Filterabfrage“

2. Klicken Sie auf **Hinzufügen**.
3. Legen Sie im Dialogfeld **Filterobjekt** fest, nach Maßgabe welcher Spalte die Daten im Ergebnisfenster gefiltert werden sollen.

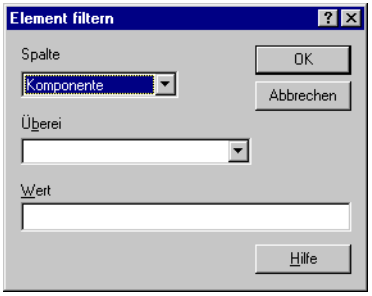


Abbildung 9-6. Dialogfeld Filterabfrage - Dialogfeld Filterobjekt

4. Verwenden Sie das Kombinationsfeld Übereinstimmung, um die Auswahlkriterien zu bestimmen.

   Sollen zwei Filter auf eine Spalte angewendet werden, können Sie z.B. für eine Spalte zwei Filter definieren, die im Feld Übereinstimmung unterschiedliche „is not“-Werte enthalten.

5. Geben Sie für den Filter einen Wert ein (beispielsweise den Namen eines Servers).
6. Klicken Sie auf **OK**, um zum Dialogfeld Filterabfrage zurückzukehren.

Der neue Filter erscheint in der Liste Aktuelle Filter. Im Ergebnisfenster ist der Name der Spalte, auf den Sie den Filter angewendet haben, in rot hervorgehoben (beispielsweise Grad), und neben dem Spaltentitel erscheint das Symbol .

7. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie erneut auf **OK** um das Dialogfeld Filterabfrage zu schließen
- Klicken Sie auf **Hinzufügen**, um einen weiteren Filter zu erstellen.

Ergänzende Informationen

- Wählen Sie im Listenfeld Aktuelle Filter einen Filter aus, und klicken Sie auf **Entfernen**, um ihn aus der Liste zu entfernen.
- Wählen Sie einen Filter aus, und klicken Sie auf **Ändern**, um seine Einstellungen zu erweitern. Die dabei verfügbaren Optionen sind dieselben, die bereits zuvor beschrieben wurden.
- Klicken Sie auf **Hilfe**, um die Hilfedatei von Log Manager zu öffnen. Kontextabhängige Hilfe ist verfügbar.

Modifizieren eines Filters

Das Modifizieren eines Filters ermöglicht es, einen vorhandenen Filter zu öffnen und dessen Einstellungen zu ergänzen. Sie haben folgende Möglichkeiten:

- Ändern der Übereinstimmungskriterien.
- Eingabe eines neuen Wertes.

Bearbeiten Sie einen Filter unter Verwendung des Dialogfelds Filterobjekt. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie Log Manager.
2. Um eine Liste der vorhandenen Filter anzuzeigen, können Sie entweder
   - Klicken Sie in der Symbolleiste auf , oder
   - aus dem Menü **Ansicht** den Befehl **Filter** wählen, um das Dialogfeld Filterabfrage (Abbildung 9-5 auf Seite 197) anzuzeigen.
3. Markieren Sie in der Liste **Aktuelle Filter** den Filter, dessen Einstellungen Sie ändern möchten, und klicken Sie dann auf **Ändern**.
4. Nehmen Sie Ihre Änderungen an dem vorhandenen Filter vor, und klicken Sie anschließend auf **OK**, um zum Dialogfeld Filterabfrage zurückzukehren.

ANMERKUNG: Sie können den in einem vorhandenen Filter zugeordneten Spaltennamen nicht ändern.

5. Führen Sie einen der folgenden Schritte aus:

- Wiederholen der Schritte 2 bis 4, um einen weiteren Filter zu bearbeiten.
- Hinzufügen eines neuen Filters
- Löschen eines Filters
- Rückkehr zu Log Manager, indem Sie erneut auf **OK** klicken.

Löschen eines Filters

Sie können einen aktiven Filter jederzeit problemlos aus Log Manager entfernen.

Um einen Filter zu löschen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie Log Manager.
2. Um eine Liste der vorhandenen Filter anzuzeigen, können Sie entweder

- Klicken Sie in der Symbolleiste auf , oder
- aus dem Menü **Ansicht** den Befehl **Filter** wählen, um das Dialogfeld Filterabfrage (Abbildung 9-5 auf Seite 197) anzuzeigen.

3. Markieren Sie in der Liste Aktuelle Filter den Filter, den Sie löschen möchten, und klicken Sie dann auf **Entfernen**.

   Der Filter wird aus Log Manager entfernt. Der zugeordnete Spaltenname im Ergebnisfenster ist anschließend nicht mehr rot hervorgehoben.

4. Führen Sie einen der folgenden Schritte aus:

- Wiederholen der Schritte 2 bis 3, um einen weiteren Filter zu entfernen.
- Hinzufügen eines neuen Filters
- Ändern der Einstellungen eines existierenden Filters
- Rückkehr zu Log Manager, indem Sie auf **OK** klicken.

Ergänzende Informationen

- Wählen Sie im Listenfeld Aktuelle Filter einen Filter aus, und klicken Sie auf **Entfernen**, um ihn aus der Liste zu entfernen.

- Wählen Sie einen Filter aus, und klicken Sie auf **Ändern**, um seine Einstellungen zu erweitern. Die dabei verfügbaren Optionen sind dieselben, die bereits zuvor beschrieben wurden.
- Klicken Sie auf **Hilfe**, um die Hilfedatei von McAfee Log Manager zu öffnen. Kontextabhängige Hilfe ist verfügbar.

Hinzufügen oder Entfernen von Spalten aus der Ansicht

Verwenden Sie das Dialogfeld **Spaltenanzeige**, um der Log Manager-Datenbank mitzuteilen, welche Spalten im Ergebnisfenster angezeigt werden sollen. Standardmäßig sind im Ergebnisfenster alle verfügbaren Spalten zu sehen.

Zum Ausblenden einer Spalte in der Ansicht führen Sie die folgenden Schritte aus:

1. Öffnen Sie Log Manager, und wählen Sie aus dem Menü **Ansicht** den Befehl **Spalten**, damit das Dialogfeld Spaltenanzeige (Abbildung 9-7) angezeigt wird.

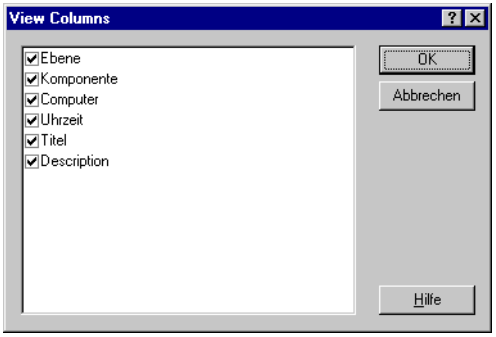


Abbildung 9-7. McAfee Log Manager - Dialogfeld „Spaltenanzeige“

2. Deaktivieren Sie dann das Kontrollkästchen neben der Spalte oder den Spalten, die ausgeblendet werden sollen.
3. Klicken Sie auf **OK**, um zum Ergebnisfenster von Log Manager zurückzukehren.

ANMERKUNG: Damit Details zu einem bestimmten Datensatz angezeigt werden, muß die Spalte Grad sichtbar sein.

Ergänzende Informationen

- Klicken Sie auf **Hilfe**, um die Hilfedatei von McAfee Log Manager zu öffnen. Kontextabhängige Hilfe ist verfügbar.
- Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, um die zugehörigen Konfigurationsoptionen anzuzeigen.

Ändern der Spaltensortierreihenfolge

Um z. B. beim Suchen nach einem bestimmten Datensatz oder beim Ermitteln eines Trends innerhalb der isolierten Objekte das Navigieren innerhalb der Datensätze im Ergebnisfenster zu erleichtern, können Sie ohne großen Aufwand die Sortierreihenfolge der Datensätze ändern, um die Anzeige jenach gewählter Spalte alphabetisch oder numerisch in auf- oder absteigender Reihenfolge neu zu arrangieren.

Um die Datensätze im Ergebnisfenster gemäß der auf- oder absteigenden Reihenfolge der Einträge einer bestimmten Spalte sortiert anzuzeigen, wählen Sie eine der folgenden Optionen:

- Markieren Sie einen Datensatz in der Spalte Grad, und wählen Sie in der Symbolleiste die Option , um die Datensätze in aufsteigender Reihenfolge ihrer Werte zu sortieren, so daß der Datenssatz mit dem kleinsten Wert am oberen Ende des Fensters angezeigt wird.
- Markieren Sie einen Datensatz in der Spalte Grad, und wählen Sie in der Symbolleiste die Option , um die Datensätze in absteigender Reihenfolge ihrer Werte zu sortieren, so daß der Datenssatz mit dem größten Wert am oberen Ende des Fensters angezeigt wird.
- Klicken Sie auf einen Spaltentitel, beispielsweise Grad, um die Datensätze in auf- oder absteigender Reihenfolge zu sortieren.
- zeigt an, daß die Spalte in aufsteigender Reihenfolge sortiert wurde, so daß der Datensatz mit dem kleinsten Wert am oberen Ende des Ergebnisfensters angezeigt wird.
- zeigt an, daß die Spalte so sortiert ist, daß sie am Anfang des Ergebnisfensters den Datensatz mit dem größten Wert anzeigt.

Ermitteln der Versionsinformationen

Um Versions- und Systeminformationen über McAfee Log Manager zu erhalten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie Log Manager, und wählen Sie eine der folgenden Möglichkeiten:
   - Klicken Sie in der Symbolleiste auf .

- Wählen Sie aus dem Menü **Hilfe** den Befehl **Info**.

2. Im Dialogfeld Info haben Sie drei Optionen:

- Um Informationen über den aktuell verwendeten Computer zu erhalten (beispielsweise die Größe des verfügbaren physischen Arbeitsspeichers), klicken Sie auf **Systeminfo**, um Microsoft Systeminfo zu öffnen.
- Um eine Verbindung mit der Network Associates-Website herzustellen und technische Auskünfte über Log Manager zu erhalten, klicken Sie auf **Technischer Support**.
- Sie können dem Dialogfeld die Versionsinformationen entnehmen. Klicken Sie auf **OK**, um zu Log Manager zurückzukehren.

Anfordern von Hilfe

Um in Log Manager Hilfe zu erhalten, wählen Sie eine der beiden folgenden Möglichkeiten:

- Öffnen Sie das Menü **Hilfe**, und wählen Sie den Befehl **Hilfethemen**, um die Hilfedatei von McAfee Log Manager zu öffnen.
- Klicken Sie in der Symbolleiste auf und anschließend auf ein Objekt auf dem Bildschirm, um kontextabhängige Hilfe zu erhalten.

Systemmonitor von GroupShield für Exchange

Mit Hilfe des Objekts **GroupShield für Exchange** im Windows NT-Systemmonitor können Sie E-Mail-Verkehr- und Viruserkennungsraten problemlos überwachen.

Führen Sie folgende Schritte aus, um den GroupShield für Exchange-Systemmonitor zu öffnen:

1. Klicken Sie in der Windows NT-Taskleiste auf **Start**, zeigen Sie auf **Programme**, und zeigen Sie dann auf **Verwaltung (Allgemein)**. Wählen Sie anschließend den Befehl **Systemmonitor**.
2. Öffnen Sie im Systemmonitor das Menü **Bearbeiten**, und wählen Sie **Diagramm erweitern** (Abbildung 9-8).

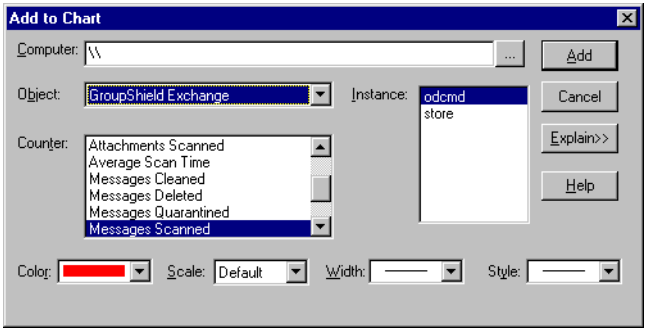


Abbildung 9-8. Windows NT Systemmonitor - Dialogfeld „Diagramm erweitern“

3. Wählen Sie im Kombinationsfeld Objekt das Objekt **GroupShield für Exchange** aus.

4. Um alle Datenquellen hinzuzufügen, halten Sie Umschalt-Taste gedrückt, klicken auf die oberste Datenquelle (**Gelöschte Anlagen**) und klicken dann auf die unterste Datenquelle (**Gefundene Viren**).

   Ab jetzt werden alle Datenquellen überwacht.

5. Damit beide Instanzen überwacht werden, halten Sie die Umschalttaste gedrückt und klicken Sie im Listenfeld Instanz auf **Bei Zugriff** und dann auf **Auf Anforderung**.

6. Klicken Sie auf **Hinzufügen** und dann auf **Fertig**.

ANMERKUNG: Das Objekt GroupShield für Exchange zählt weiter, solange Auf Anforderung ausgeführt wird. Daher meldet die Datenquelle eine größere Anzahl gescannter Nachrichten, als sich im Microsoft Exchange-Informationsspeicher befindet. Um die Datenquelle zurückzusetzen, beenden Sie die GroupShield für Exchange-Dienste und starten diese erneut. Die Software schützt jedoch nicht gegen Virusinfektionen, wenn die Virenschutzdienste angehalten sind.

Quarantänemethoden 10

Ihre McAfee-Virenschutz-Software kann blockierte oder infizierte E-Mail-Objekte an einen sicheren Quarantäneort auf Ihrem Microsoft Exchange-Server senden. Ein isoliertes Objekt kann jederzeit angezeigt werden, um zu ermitteln, warum es isoliert wurde und um zu entscheiden, ob es gelöscht, gesäubert oder an den betreffenden Empfänger oder einen anderen E-Mail-Administrator in Ihrer Organisation gesendet werden soll.

ACHTUNG: McAfee empfiehlt dringend, ein isoliertes Objekt nicht an andere Benutzer, ausgenommen das Network Associates AVERT-Virusforschungslabor, zu senden. Senden Sie es erst dann an andere Benutzer, wenn es gesäubert wurde und nachgewiesenerweise virenfrei ist.

GroupShield für Exchange unterstützt zwei Quarantänemethoden:

- Die McAfee Quarantine Manager-Datenbank
- Das Quarantäneverzeichnis

Welche Quarantänemethode verwendet wird, wird bei der Installation von GroupShield für Exchange festgelegt. Sie können die Methode und den entsprechenden Speicherort jedoch auch nachträglich ändern. Dazu verwenden Sie die Registerkarte **Administration** des Serverdaministrationsmoduls von GroupShield für Exchange. In “Auswählen einer Isolierungsmethode und eines Quarantäneortes“ auf Seite 116 finden Sie diesbezügliche Informationen.

Andere Quarantäneaktionen werden an anderen Stellen in der Serververwaltungskonsole GroupShield-Eigenschaften festgelegt.

- Weitere Informationen zum Blockieren und Isolieren von E-Mail-Nachrichten finden Sie unter “Blockieren von Anlagen bestimmten Typs“ auf Seite 66.
- Weitere Informationen zu Quarantäneaktionen für Scanvorgänge bei Zugriff finden Sie unter “Festlegen der Aktionen zur Behandlung aufgespürter Viren“ auf Seite 65.
- Weitere Informationen zu Quarantäneaktionen für Scanvorgänge auf Anforderung finden Sie unter “GroupShield für Exchange-Aktionen bei Viruserkennung“ auf Seite 79.

McAfee Quarantine Manager - Einführung

Die Quarantine Manager-Datenbank enthält detaillierte Informationen über blockierte oder infizierte Objekte, die von GroupShield für Exchange entdeckt wurden. Mit dem Quarantine Manager können Sie:

- Eine Liste der momentan isolierten Objekte anzeigen und Details zu jedem einzelnen Eintrag abrufen. Bei Bedarf können Sie Filter anwenden, um die Objekte für Analysen weiter zu sortieren.
- Eine „Momentaufnahme" der Quarantine Manager-Datenbank speichern, um diese zu archivieren oder an die Support-Dienste von Network Associates zu übermitteln.
- Mit Benutzern die Gründe klären, warum ein Objekt isoliert wurde. Filtern Sie dazu die Spalte **QNumber** nach der vom Benutzer angegebenen Ticket-Nummer, und rufen Sie dann Details zu dem isolierten Objekt ab.
- Eine infizierte Nachricht oder Anlage löschen.
- Die gesamte Quarantänedatenbank aus Ihrem System löschen.

  Ein solcher Vorgang wirkt sich auf keine der archivierten Sichten der Quarantänedatenbank aus.
- Archivierte Quarantänedatenbanken öffnen, um Informationen zu vergleichen.
- Eine Anlage auf dem Desktop des lokalen Computers speichern, wo sie unter Verwendung des lokalen Virenschutzprogramms gesäubert werden kann.
- Ein Objekt an einen anderen Benutzer, z.B. den vorgesehenen Empfänger, senden.

ANMERKUNG: McAfee empfiehlt Ihnen, darauf zu achten, eine isolierte Anlage erst dann an einen anderen Benutzer weiterzuleiten, wenn sie zuvor von Viren gesäubert wurde.

- Ein Objekt, von dem Sie annehmen, daß es ein neues Virus ist, an die Network Associates-Forschungslabors senden. Siehe „Melden neuer Posten für Virenschutzdatendateien" auf Seite xxi.

Quarantine Manager besteht aus drei verschiedenen Bereichen für Konfiguration und Informationsanzeige.

- Eine Beschreibung der in der Menüleiste verfügbaren Optionen finden Sie auf Seite 207
- Eine Beschreibung der in der Symbolleiste verfügbaren Optionen finden Sie auf Seite 209
- Eine Beschreibung des Inhalts des Ergebnisfensters finden Sie auf Seite 210.

Die Benutzeroberfläche von Quarantine Manager

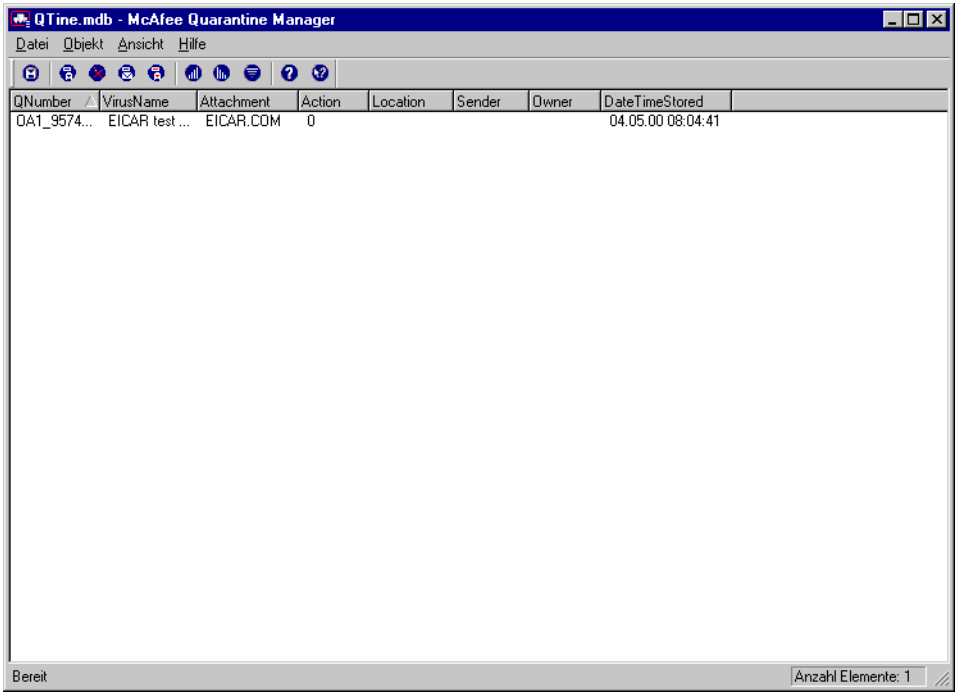

QTine.mdb - McAfee Quarantine Manager
Datei Objekt Ansicht Hilfe
QNumber VirusName Attachment Action Location Sender Owner DateTimeStored
0A1_9574... EICAR test ... EICAR.COM 0 04.05.00 08:04:41
Bereit
Anzahl Elemente: 1

Abbildung 10-1. McAfee Quarantine Manager-Benutzeroberfläche

Die Menüleiste

Verwenden Sie die Menüleiste, um Quarantine Manager zu konfigurieren und Informationen über die einzelnen aufgezeichneten Ereignisse anzuzeigen.

Das Menü „Datei“

- Der Befehl **Öffnen** öffnet eine zuvor gespeicherte Quarantine Manager-Datenbank oder eine Quarantäne-Datenbank, die auf einem anderen Server abgelegt wurde.

ANMERKUNG: Verwenden Sie die **Netzwerkumgebung**, um eine Quarantine Manager-Datenbank auf einem anderen Server zu starten. Möglicherweise benötigen Sie dazu einen Benutzernamen und ein Kennwort.

Mit dem Befehl **Speichern unter** wird die aktuelle Ansicht von Quarantine Manager zu Analyse- oder Archivierungszwecken unter einem anderen Dateinamen abgelegt.

ANMERKUNG: Der Befehl **Speichern unter** dient dazu, eine „Momentaufnahme" der Datenbank zu speichern, um sie beispielsweise an den Support von Network Associates zu senden. Die im CSV-Format gespeicherte Datei kann in Microsoft Excel importiert und dort analysiert und ausgewertet werden.

- Der Befehl **Gefiltertes Protokoll löschen** entfernt gefilterte Datensätze aus der Quarantine Manager-Datenbank

  Dieser Vorgang kann nicht rückgängig gemacht werden.

- Der Befehl **Ganzes Protokoll löschen** entfernt alle Datensätze aus der Quarantine Manager-Datenbank

  Dieser Vorgang kann nicht rückgängig gemacht werden.

- **Beenden** schließt das Quarantine Manager-Programm

Das Menü „Objekt"

- Der Befehl **Löschen** entfernt den gewählten Datensatz aus dem Ergebnisfenster von Quarantine Manager.

- Mit dem Befehl **Speichern** können Sie den gewählten Datensatz in einem Ordner Ihres lokalen Computersystems (beispielsweise auf dem Desktop) ablegen, wo Sie versuchen können, das Objekt unter Verwendung Ihres lokalen Virenschutzprogramms zu säubern, oder Sie können das Objekt auf einem Netzwerklaufwerk ablegen, von dem aus es für den ursprünglichen Adressaten erreichbar wird.

  McAfee empfiehlt, daß Sie ein isoliertes Objekt erst dann an einen anderen Benutzer senden, nachdem Sie die Virenfreiheit des Objekts überprüft haben.

- Der Befehl **Senden an** übermittelt ein Objekt an einen anderen Benutzer (z. B. den ursprünglichen Adressaten), sofern die Virenfreiheit des Objekts überprüft worden ist.

- Der Befehl **Senden an Avert** sendet das gewählte Objekt an die Forschungslabors von Network Associates. In "Melden neuer Posten für Virenschutzdatendateien" auf Seite xxi finden Sie diesbezügliche Informationen.

Das Menü „Ansicht"

- Der Befehl **Aktualisieren** fügt Datensätze hinzu, die seit dem Laden der Quarantine Manager-Datenbank neu protokolliert wurden

- Der Befehl **Filter** erstellt, ändert und löscht Filter
- Der Befehl **Spalten** dient dazu, festzulegen, welche der Spalten im Ergebnisfenster sichtbar sein sollen

  Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, um die verfügbaren Konfigurationsoptionen anzuzeigen.
- Der Befehl **Details** zeigt Informationen über ein isoliertes Objekt an.

  Damit die Detailübersicht für ein Objekt angezeigt werden kann, muß die Spalte QNumber im Ergebnisfenster sichtbar sein.

Der untere Teil des Menüs Ansicht enthält Optionen für die einzelnen Quarantine Manager-Komponenten. Klicken Sie auf einen Eintrag, um bestimmte Komponenten innerhalb der Ansicht ein- oder auszublenden.

Das Menü „Hilfe“

Im Menü Hilfe können Sie die folgenden Optionen wählen:

- Der Befehl **Hilfethemen** öffnet die Hilfedatei für McAfee Quarantine Manager.
- Mit dem Befehl **Info** wird ein Dialogfeld mit Copyright-Informationen zu Quarantine Manager und Systeminformationen über den aktuellen Microsoft Exchange-Server geöffnet. Das Dialogfeld ermöglicht außerdem eine Verbindung mit der Network Associates-Website für technischen Support.

Klicken Sie im Dialogfeld Info auf **OK**, um zu Quarantine Manager zurückzukehren.

Die Symbolleiste

Verwenden Sie die Symbolleiste, um die Ansicht für Quarantine Manager festzulegen, Copyright-Informationen anzuzeigen und Hilfe zu erhalten. Folgende Optionen sind verfügbar:

speichert die aktuelle Ansicht von Quarantine Manager in einer anderen Datei.

Die Option Speichern unter dient dazu, eine „Momentaufnahme“ der Datenbank zu speichern, um sie beispielsweise an den Support von Network Associates zu senden. Die im .CSV-Format gespeicherte Datei kann in Microsoft Excel importiert und dort analysiert und ausgewertet werden.

Speichert das gewählte Objekt im Netzwerk an einer Stelle Ihrer Wahl, sodaß andere Benutzer es öffnen können.

löscht das ausgewählte Objekt aus der Quarantäne-Datenbank.

gibt das gewählte Objekt aus der Quarantäne-Datenbank frei und startet Ihr E-Mail-Clientprogramm.

Senden Sie das Objekt z. B. an den ursprünglichen Adressaten, wenn Sie das Objekt überprüft haben und festgestellt haben, daß es nicht von einem Virus infiziert ist. Weitere Informationen zum Entfernen eines Virus aus einem isolierten Objekt finden Sie unter “Säubern einer infizierten Datei in der Quarantäne-Datenbank“ auf Seite 215.

sendet das ausgewählte Objekt zum Testen an die AVERT-Labors von Network Associates.

Sortiert die Datensätze so, daß der kleinste Datensatz am oberen Ende des Ergebnisfensters angezeigt wird.

Sortiert die Datensätze so, daß der größte Datensatz am oberen Ende des Ergebnisfensters angezeigt wird.

Öffnet das Dialogfeld **Filterabfrage**, in dem Sie Protokollfilter definieren, ändern oder löschen können.

öffnet das Dialogfeld Info von Quarantine Manager.

Das Fenster zeigt die Copyright-Details zu Quarantine Manager sowie Systeminformationen über den aktuellen Server an und ermöglicht eine Verbindung mit der Network Associates-Website für den technischen Support. Klicken Sie im Dialogfeld Info auf **OK**, um zum Quarantine-Manager zurückzukehren.

startet die Direkthilfe. Klicken Sie auf diese Schaltfläche und anschließend auf ein Objekt auf dem Bildschirm, um kontextabhängige Hilfe zu erhalten.

Das Ergebnisfenster

Das Ergebnisfenster zeigt Informationen über isolierte Objekte an.

- **QNumber** zeigt die Ticket-Nummer an, die dem isolierten Objekt zugeordnet wurde. Sofern diese Nummer angegeben ist, erhält der ursprüngliche Adressat eine E-Mail-Anlage mit der Bezeichnung ALERT.TXT, die die isolierte Anlage mit der Ticket-Nummer ersetzt. Der Empfänger kann dem Administrator diese Ticket-Nummer angeben, um herauszufinden, warum die Anlage isoliert wurde und welche Aktionen erfolgten, ob die Anlage z. B. gelöscht wurde.
- **Virusname** gibt den Namen des entdeckten Virus an, sofern dies möglich ist. Diese Spalte bleibt leer, wenn das Objekt aufgrund seiner Erweiterung oder des Inhalts isoliert wurde.
- **Anlage** gibt den Namen der isolierten Anlage an.
- **Aktion** gibt an, ob das infizierte Objekt isoliert oder blockiert wurde.

- **Speicherort** informiert über den Verbleib des infizierten Objekts. Der Speicherort wird nur nach einem Scanvorgang auf Anforderung gemeldet.
- **Absender** gibt das Postfach an, das das isolierte Objekt gesendet hat.
- **Besitzer** bezeichnet den ursprünglichen Adressaten des Objekts, sofern dieser ermittelbar ist.
- **Speicherungsdatum** gibt Datum und Zeitpunkt der Isolierung des Objekts an.

Ergänzende Informationen

- Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, um die zugehörigen Konfigurationsoptionen anzuzeigen.
- Doppelklicken Sie auf ein Objekt in der Spalte **QNumber**, um Informationen zu diesem Objekt anzuzeigen.
- Ein in Rot hervorgehobener Spaltenname mit dem Symbol zeigt an, daß dieser Spalte ein Filter zugeordnet wurde.
- zeigt an, daß die Spalte am oberen Ende des Ergebnisfensters den Datensatz mit dem kleinsten Wert enthält.
- zeigt an, daß die Spalte am oberen Ende des Ergebnisfensters den Datensatz mit dem größten Wert enthält.
- Verwenden Sie das Menü **Ansicht**, um Typ und Darstellung der im Ergebnisfenster sichtbaren Informationen zu ändern.

Verwenden von McAfee Quarantine Manager

Öffnen von Quarantine Manager

Sie können die Quarantäne-Datenbank aus der Serververwaltungskonsole GroupShield-Eigenschaften anzeigen.

So starten Sie die Quarantäne-Datenbank

1. Öffnen Sie die Serververwaltungskonsole GroupShield-Eigenschaften.

   Die Registerkarte Administration wird als Standardseite angezeigt.

2. Wählen Sie im Feld **Standort Quarantänebereich** das Optionsfeld **Datenbank verwenden** (wenn dieses nicht bereits gewählt ist), und klicken Sie dann auf Ansicht, um McAfee Quarantine Manager anzuzeigen (Abbildung 10-1 auf Seite 207).

   WICHTIG: McAfee empfiehlt, die Quarantäne-Datenbank nicht aus der Windows NT Explorer-Ansicht heraus zu öffnen.

Speichern der Quarantäne-Datenbank

Sie können eine „Momentaufnahme“ der Datenbank in einer Datei ablegen, um sie beispielsweise an den Support von Network Associates zu senden oder zu archivieren.

Führen Sie zum Speichern einer Kopie der Quarantäne-Datenbankansicht die folgenden Schritte aus:

1. Öffnen Sie McAfee Quarantine Manager, und wählen Sie eine der folgenden Möglichkeiten:

- Klicken Sie in der Symbolleiste auf .
- Wählen Sie im Menü **Datei** den Befehl **Speichern unter**.

2. Wechseln Sie im Dialogfeld Speichern unter (Abbildung 10-2) zu dem Ordner auf Ihrem Computer oder im Netzwerk, in dem die Datenbank abgelegt werden soll.

Abbildung 10-2. McAfee Quarantine Manager - Dialogfeld „Speichern unter“

3. Geben Sie gegebenenfalls einen eindeutigen Dateinamen in das dafür vorgesehene Textfeld ein.

   McAfee empfiehlt, bei jeder Speicherung des Datenbankzustands jeweils einen anderen eindeutigen Dateinamen zu wählen, um eine spätere Identifizierung zu erleichtern.

4. Klicken Sie auf **Speichern**.

ANMERKUNG: Einer gespeicherten Kopie der Datenbank werden keine neuen Datensätze mehr hinzugefügt, nachdem der Speicherungsvorgang abgeschlossen ist.

Öffnen einer archivierten Quarantäne-Datenbank

Die Quarantäne-Datenbank kann zu Archivierungszwecken unter einem anderen Dateinamen auf Ihrem Computer oder im Netzwerk gespeichert werden.

Um eine archivierte Datenbank zu öffnen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Dienstprogramm Quarantine Manager, und wählen Sie aus dem Menü **Datei** die Option **Öffnen**.
2. Wechseln Sie zu demjenigen Ordner auf Ihrem Computer oder im Netzwerk, in dem die archivierte Kopie der Datenbank abgelegt wurde.
3. Markieren Sie im Dialogfeld Öffnen (Abbildung 10-3) den Namen der Datei, und klicken Sie dann auf **Öffnen**.

Abbildung 10-3. McAfee Quarantine Manager - Dialogfeld „Öffnen“

Übermitteln von Objekten, die durch neue Virusarten infiziert wurden, an Network Associates

Da die Forscher von McAfee immer bestrebt sind, Ihnen für den Schutz Ihrer Systeme jeweils effektive und nach dem neuesten Stand der Technik arbeitende Werkzeuge zur Hand zu geben, sind wir sehr daran interessiert, daß Sie uns über alle neuen Java-Klassen, ActiveX-Steuerelemente, zweifelhaften Websites oder Viren berichten, die die von Ihnen verwendete Software nicht zu entdecken vermag.

Mit McAfee QuarantineManager können mögliche neue Viren oder verdächtige Objekte problemlos an die AVERT-Labors von Network Associates zu senden.

Führen Sie dazu einfach die folgenden Schritte aus:

1. Öffnen Sie McAfee QuarantineManager, und wählen Sie im Ergebnisfenster das Objekt, das Sie versenden möchten.
2. Wählen Sie anschließend eine der folgenden Optionen:

- Klicken Sie in der Symbolleiste auf .
- Wählen Sie aus dem Menü **Objekt** die Option **Senden an Avert**.

  Anschließend startet automatisch Ihr E-Mail-Clientprogramm mit einer neu erstellten E-Mail-Nachricht, in der als Empfänger schon Avert@nai.com eingetragen ist und in dessen Textfeld das isolierte Objekt bereits eingefügt worden ist.

Senden isolierter Objekte an andere Benutzer

Das Dienstprogramm QuarantineManager ermöglicht es Ihnen, ein isoliertes Objekt zu inspizieren und zu entscheiden, ob sich das Objekt in einem sicheren oder sonstwie geeigneten Zustand befindet, um es mit dem Befehl Senden an per E-Mail an einen anderen Benutzer zu senden, beispielsweise den ursprünglichen Adressaten oder einen anderen Administrator.

So senden Sie ein isoliertes Objekt per E-Mail an einen anderen Benutzer

1. Öffnen Sie das Dienstprogramm QuarantineManager, und wählen Sie eine der folgenden Möglichkeiten:

- Klicken Sie in der Symbolleiste auf .
- Wählen Sie aus dem Menü **Objekt** die Option **Senden an**.

2. Anschließend startet automatisch Ihr E-Mail-Clientprogramm mit einer neu erstellten E-Mail-Nachricht, in deren Textfeld das isolierte Objekt bereits eingefügt wurde.

3. Fügen Sie die E-Mail-Adresse des gewünschten Adressaten ein, und versenden Sie die Nachricht in der üblichen Weise.

Säubern einer infizierten Datei in der Quarantäne-Datenbank

Um ein in der Quarantäne-Datenbank abgelegtes Objekt von Viren zu säubern, führen Sie die folgenden Schritte aus:

1. Öffnen Sie Quarantine Manager. Wählen Sie im Ergebnisfenster das Objekt aus, das gesäubert werden soll.

2. Klicken Sie in der Symbolleiste auf , oder wählen Sie aus dem Menü **Objekt** die Option **Speichern**. Wählen Sie im Dialogfeld Speichern unter im Kombinationsfeld Speichern in den Eintrag **Desktop**, und klicken Sie dann auf **Speichern**.

3. Minimieren Sie anschließend die Ansicht von McAfee Quarantine Manager, und öffnen Sie Ihr Desktop-Antivirenschutzprogramm, beispielsweise McAfee VirusScan*.

   Weiterführende Anweisungen entnehmen Sie bitte der Dokumentation für Ihr Desktop-Virenschutz-Programm.

   Das Programm durchsucht die Datei nach Viren und versucht, diese aus der Datei zu entfernen. Wenn dieser Versuch erfolgreich verläuft, löschen Sie das Objekt auf dem Desktop und kehren zu Quarantine Manager zurück, wo Sie das Objekt an den ursprünglichen Adressaten weiterleiten können. Klicken Sie in der Symbolleiste auf , und führen Sie dann die unter “Senden isolierter Objekte an andere Benutzer“ auf Seite 214 genannten Schritte durch.

Hinzufügen eines neuen Filters

Verwenden Sie das Dialogfeld Filterabfrage, um Filter für die Quarantine Manager-Datenbank zu definieren, zu modifizieren und zu entfernen. Ein Filter ersetzt die im Ergebnisfenster sichtbaren Datensätze durch eine Gruppe spezifischerer Datensätze. Dabei werden die Datensätze, die nicht den von Ihnen festgelegten Parametern entsprechen, aus der Ansicht entfernt. Es können mehrere Filter auf eine Spalte angewendet werden, und es können mehrere Spalten gleichzeitig gefiltert werden.

Um einen neuen Filter hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Quarantine Manager-Datenbank, und wählen Sie eine dieser Optionen, um das Dialogfeld Filterabfrage zu öffnen (Abbildung 10-4 auf Seite 216):

- Klicken Sie in der Symbolleiste auf .
- Wählen Sie aus dem Menü **Ansicht** den Befehl **Filter**.

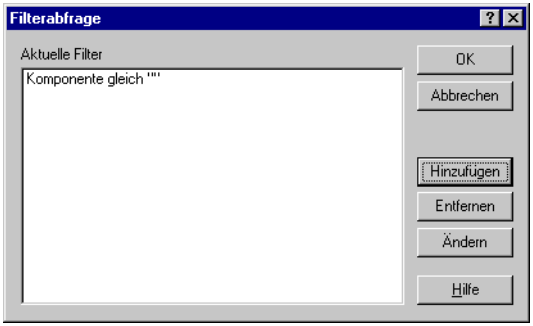


Abbildung 10-4. McAfee Quarantine Manager - Dialogfeld „Filterabfrage“

2. Klicken Sie auf **Hinzufügen**.
3. Legen Sie im Dialogfeld Filterobjekt fest, nach Maßgabe welcher Spalte die Daten im Ergebnisfenster gefiltert werden sollen.

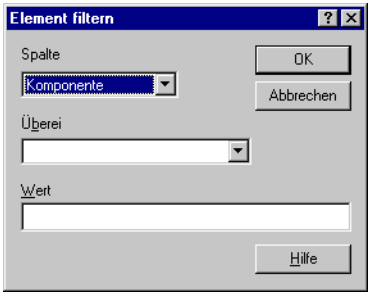


Abbildung 10-5. Dialogfeld „Filterabfrage“ - Dialogfeld „Filterobjekt“

4. Verwenden Sie das Kombinationsfeld Übereinstimmung, um die Auswahlkriterien zu bestimmen.

Sollen zwei Filter auf eine Spalte angewendet werden, können Sie z.B. für eine Spalte zwei Filter definieren, die im Feld Übereinstimmung unterschiedliche „is not“-Werte enthalten.

5. GebenSiefürdenFiltereinenWertein(beispielsweisedenNameneinesServers).
6. Klicken Sie auf **OK**, um zum Dialogfeld Filterabfrage zurückzukehren.

   DerneueFiltererscheintinderListeAktuelleFilter.DerNamederSpalte,derSie denFilterzugeordnethaben,wirdimErgebnisfensterrothervorgehoben,zum BeispielQNumber,undistimSpaltentiteldurchdasSymbol gekennzeichnet.
7. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie erneut auf **OK** um das Dialogfeld Filterabfrage zu schließen
- Klicken Sie auf **Hinzufügen**, um einen weiteren Filter zu erstellen.

Ergänzende Informationen

- Wählen Sie im Listenfeld Aktuelle Filter einen Filter aus, und klicken Sie auf **Entfernen**, um ihn aus der Liste zu entfernen.
- WählenSieeinenFilteraus,undklickenSieauf**Ändern**,umseineEinstellungenzu erweitern. Die dabei verfügbaren Optionen sind dieselben, die bereits zuvor beschrieben wurden.
- Klicken Sie auf **Hilfe**, um die Hilfedatei für McAfee Quarantine Manager zu öffnen. Es steht kontextabhängige Hilfe zur Verfügung.

Modifizieren eines Filters

DasModifiziereneinesFiltersermöglichtes,einenvorhandenenFilterzuöffnenund dessen Einstellungen zu ergänzen. Sie haben folgende Möglichkeiten:

- Ändern der Übereinstimmungskriterien
- Eingabe eines neuen Wertes.

Bearbeiten Sie einen Filter unter Verwendung des Dialogfelds Filterobjekt. Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie Quarantine Manager.
2. Um eine Liste der vorhandenen Filter anzuzeigen, können Sie entweder:

- in der Symbolleiste wählen, oder
- Wählen Sie aus dem Menü **Ansicht** den Befehl **Filter**.

3. Markieren Sie in der Liste Aktuelle Filter im Dialogfeld **Filterabfrage** den Filter, dessen Einstellungen Sie ändern möchten, und klicken Sie dann auf **Ändern**.

4. Ändern Sie den vorhandenen Filter wie gewünscht im Dialogfeld Filterobjekt (Abbildung 10-5 auf Seite 216), und klicken Sie dann auf **OK**, um zum Dialogfeld Filterabfrage zurückzukehren.

ANMERKUNG: Sie können den in einem vorhandenen Filter zugeordneten Spaltennamen nicht ändern.

---

5. Führen Sie einen der folgenden Schritte aus:

- Wiederholen der Schritte 2 bis 4, um einen weiteren Filter zu bearbeiten
- Hinzufügen eines neuen Filters
- Löschen eines Filters
- Klicken Sie dann erneut auf **OK**, um zu Quarantine Manager zurückzukehren.

Löschen eines Filters

Sie können einen aktiven Filter jederzeit problemlos aus Quarantine Manager entfernen.

Um einen Filter zu löschen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie Quarantine Manager.

2. So zeigen Sie eine Liste der vorhandenen Filter im Dialogfeld Filterabfrage (Abbildung 10-4 auf Seite 216) an:

- Klicken Sie in der Symbolleiste auf , oder
- Wählen Sie aus dem Menü **Ansicht** den Befehl **Filter**.

3. Markieren Sie in der Liste Aktuelle Filter den Filter, den Sie löschen möchten, und klicken Sie dann auf **Entfernen**. Der Filter wird aus Quarantine Manager entfernt. Der zugeordnete Spaltenname im Ergebnisfenster ist anschließend nicht mehr rot hervorgehoben.

4. Führen Sie einen der folgenden Schritte aus:

- Wiederholen der Schritte 2 bis 3, um einen weiteren Filter zu entfernen
- Hinzufügen eines neuen Filters
- Ändern der Einstellungen eines existierenden Filters
- Klicken Sie dann auf **OK**, um zu Quarantine Manager zurückzukehren.

Hinzufügen oder Entfernen von Spalten zur/aus der Ansicht

Verwenden Sie das Dialogfeld **Spaltenanzeige**, um der Quarantine Manager-Datenbank mitzuteilen, welche Spalten im Ergebnisfenster angezeigt werden sollen. Standardmäßig sind im Ergebnisfenster alle verfügbaren Spalten zu sehen.

Zum Ausblenden einer Spalte in der Ansicht führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Dienstprogramm Quarantine Manager, und wählen Sie aus dem Menü **Ansicht** die Option **Spalten**.
2. Deaktivieren Sie im Dialogfeld Spaltenanzeige (Abbildung 10-6) das Kontrollkästchen neben der Spalte / den Spalten, die ausgeblendet werden soll(en).

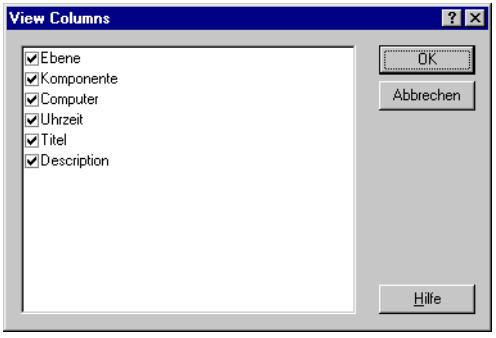


Abbildung 10-6. McAfee Quarantine Manager - Dialogfeld „Spaltenanzeige“

3. Klicken Sie auf **OK**, um zum Ergebnisfenster von Quarantine Manager zurückzukehren.

Ergänzende Informationen

- Klicken Sie auf **Hilfe**, um die Hilfedatei für Quarantine Manager zu öffnen. Innerhalb des Dialogfelds ist kontextabhängige Hilfe verfügbar.
- Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, um die zugehörigen Konfigurationsoptionen anzuzeigen.

Anzeigen von Details zu einem Datensatz

Verwenden Sie das Fenster Datensatzdetails, um Informationen über ein ausgewähltes isoliertes Objekt zu erhalten.

Führen Sie hierzu die folgenden Schritte durch:

1. Öffnen Sie das Quarantine Manager-Dienstprogramm, und markieren Sie den Datensatz, der angezeigt werden soll.

   Die Spalte **QNumber** muß im Ergebnisfenster sichtbar sein. Nur dann kann ein Datensatz ausgewählt werden. Siehe “Hinzufügen oder Entfernen von Spalten zur / aus der Ansicht“ auf Seite 219.

2. Wählen Sie **Details** aus dem Menü **Ansicht**, um das Dialogfeld Datensatzdetails anzuzeigen (Abbildung 10-7).

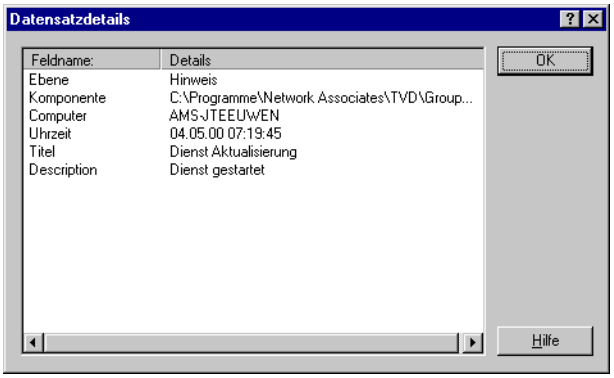


Abbildung 10-7. McAfee Quarantine Manager - Dialogfeld „Datensatzdetails“

3. Klicken Sie auf **OK**, um zum Ergebnisfenster von Quarantine Manager zurückzukehren.

Ermitteln der Versionsinformationen

Um Versions- und Systeminformationen über das McAfee Quarantine Manager-Dienstprogramm zu erhalten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie Quarantine Manager, und wählen Sie eine der folgenden Möglichkeiten:

- Klicken Sie in der Symbolleiste auf .
- Wählen Sie aus dem Menü **Hilfe** die Option **Info**.

2. Im Dialogfeld **Info** haben Sie drei Optionen:

- Um Informationen über den aktuell verwendeten Computer zu erhalten (beispielsweise die Größe des verfügbaren physischen Arbeitsspeichers), klicken Sie auf **Systeminfo**, um Microsoft Systeminfo zu öffnen.
- Um eine Verbindung mit der Network Associates-Website herzustellen und technische Auskünfte über Quarantine Manager zu erhalten, klicken Sie auf **Technischer Support**.
- Im Dialogfeld sind die Versionsinformationen angegeben. Klicken Sie auf **OK**, um zu Quarantine Manager zurückzukehren.

Ändern der Spaltensortierreihenfolge

Wenn Sie das Navigieren durch die Datensätze im Ergebnisfenster beim Suchen nach einem bestimmten Datensatz oder beim Ermitteln eines Trends in der Liste isolierter Objekte erleichtern möchten, können Sie ohne großen Aufwand die Sortierreihenfolge der Datensätze ändern und die Anzeige je nach gewählter Spalte alphabetisch oder numerisch in auf- oder absteigender Reihenfolge neu anordnen.

Um die Datensätze im Ergebnisfenster gemäß der auf- oder absteigenden Reihenfolge der Einträge einer bestimmten Spalte sortiert anzuzeigen, wählen Sie eine der folgenden Optionen:

- Markieren Sie einen Datensatz in der Spalte QNumber, und wählen Sie aus der Symbolleiste, um die Datensätze in aufsteigender Reihenfolge ihrer Werte zu sortieren, so daß der Datensatz mit dem kleinsten Wert am oberen Ende des Fensters angezeigt wird.
- Markieren Sie einen Datensatz in der Spalte QNumber, und wählen Sie aus der Symbolleiste, um die Datensätze in absteigender Reihenfolge ihrer Werte zu sortieren, so daß der Datensatz mit dem größten Wert am oberen Ende des Fensters angezeigt wird.
- Klicken Sie auf einen Spaltentitel, beispielsweise QNumber, um die Datensätze in auf- oder absteigender Reihenfolge zu sortieren.

zeigt an, daß die Spalte in aufsteigender Reihenfolge sortiert wurde, so daß der Datensatz mit dem kleinsten Wert am oberen Ende des Ergebnisfensters angezeigt wird.

zeigt an, daß die Spalte so sortiert ist, daß sie am Anfang des Ergebnisfensters den Datensatz mit dem größten Wert anzeigt.

Anfordern von Hilfe

Um im Quarantine Manager-Dienstprogramm Hilfe zu erhalten, wählen Sie eine der beiden folgenden Möglichkeiten:

- Öffnen Sie das Menü **Hilfe**, und wählen Sie die Option **Hilfethemen**, um die Hilfedatei von McAfee Quarantine Manager zu öffnen.
- Klicken Sie in der Symbolleiste auf und anschließend auf ein Objekt auf dem Bildschirm, um kontextabhängige Hilfe zu erhalten.

Das Quarantäneverzeichnis

Das Quarantäneverzeichnis speichert blockierte oder infizierte E-Mail-Nachrichten und deren Anlagen an einem sicheren Ort in Ihrem System. Das Quarantäneverzeichnis enthält die Details zu jedem isolierten Element, z.B. den Namen der Datei und den Namen des Virus, in einer Header-Datei. Die Header-Datei enthält auch die isolierte Anlage.

WICHTIG: McAfee empfiehlt, daß Sie mit allen isolierten Anlagen sehr vorsichtig umgehen und diese nicht an andere Personen weiterleiten, es sei denn, Sie sind sich absolut sicher, daß die jeweilige Anlage nicht infiziert ist.

Zum Öffnen blockierter oder infizierter Objekte aus dem Quarantäneverzeichnis führen Sie die folgenden Schritte aus:

1. Wechseln Sie zu demjenigen Ordner in Ihrem Netzwerk, den Sie als Standort für das Quarantäneverzeichnis festgelegt haben.
2. Doppelklicken Sie auf ein Element, um eine Beispiel-E-Mail-Nachricht anzuzeigen, die die isolierte Anlage enthält.

Ergänzende Informationen

- Leiten Sie die Anlage mit Hilfe Ihrer E-Mail-Client-Software an einen anderen Administrator weiter.
- McAfee empfiehlt dringend, ein isoliertes Objekt nicht an andere Benutzer, ausgenommen das Network Associates AVERT-Virusforschungslabor, zu senden. Senden Sie es erst dann an andere Benutzer, wenn es gesäubert wurde und nachgewiesenerweise virenfrei ist.

Das Dienstprogramm Outbreak Manager 11

Schützen vor Virusepidemien

McAfee hat ein leistungsstarkes Produkt zur Überwachung von Virusepidemien, das Dienstprogramm Outbreak Manager, in Ihr Virenschutzprogramm integriert. Dieses innovative Dienstprogramm bietet zusätzlichen Schutz vor unerwarteten Virusangriffen in großem Stil (Virusepidemien) und erweitert auf diese Weise den Virenschutz Ihrer Organisation.

Ziel des Dienstprogramms Outbreak Manager ist es, Virusepidemien intuitiv zu entdecken und darauf zu reagieren. Das Programm bietet kontinuierlich reagierenden Schutz auf der Grundlage einer Auswahl von Regeln, die Sie selbst festlegen können. Es kann über Virusepidemien benachrichtigen oder automatisierte Reaktionen veranlassen. Je nachdem, welches Virenschutzprogramm Sie installiert haben, steht gegebenenfalls eine weitere Option zur Verfügung, mit der Sie Anwesenheitszeiten (beispielsweise im Büro) angeben können. Dies ermöglicht es dem Dienstprogramm Outbreak Manager, bei Ausbruch von Virusepidemien automatische Reaktionen zu veranlassen, *wenn Sie zu diesen Zeiten nicht in Ihrem Büro sind oder nicht an Ihrem Schreibtisch sitzen*.

Funktionsübersicht

Virusepidemien können entstehen, wenn zahlreiche identische Anlagen (die ein Virus enthalten) in kurzer Zeit mithilfe einer großen Zahl separater E-Mail-Nachrichten über das Internet verbreitet werden. Bei einer großflächigen Epidemie führt das hohe Aufkommen infizierter E-Mail-Nachrichten dazu, daß innerhalb von kurzer Zeit eine Vielzahl von Kopien der Anlage eine Organisation erreichen können.

Erkennen einer Epidemie

Das Dienstprogramm Outbreak Manager ist in der Lage, Virusepidemien auf der Grundlage von Auslösern zu identifizieren, die Sie für die Ausbruchregeln angeben. Je nach eingesetztem Virenschutzprogramm kann eine größere oder kleinere Auswahl der folgenden Kriterien überwacht werden:

- Mehrere Viren während eines vorgegebenen Zeitraums.
- Mehrere identische Viren während eines vorgegebenen Zeitraums.
- Mehrere identische Anlagen während eines vorgegebenen Zeitraums.
- Mehrere identische Anlagentypen während eines vorgegebenen Zeitraums.

Schnelle Reaktion

Wenn das Dienstprogramm Outbreak Manager unter Verwendung der Regelauslöser, die Sie zur Identifizierung solcher Fälle definiert haben, eine Virusepidemie entdeckt, kann es auf zweierlei Weise reagieren:

- **Manuelle Aktionen, die eine Aktion des Benutzers erfordern**

  Das Dienstprogramm Outbreak Manager zeigt ein Meldungsfeld an, das Sie über die Virusepidemie informiert. Sie können dann die erforderlichen Aktionen aus einer Liste wählen, die Sie zuvor für die Regel konfiguriert haben, welche die Virusepidemie identifiziert hat.

- **Automatische Aktionen**

  Outbreak Manager führt automatisch die Aktionen durch, die Sie für die Regel festgelegt haben, welche die Virusepidemie identifiziert. Sie können Ausweitungszeiten für die verschiedenen Aktionen festlegen, so daß diese nur dann erfolgen, wenn die Regel auch nach Ablauf der Ausweitungszeit weiterhin Virusepidemien feststellt.

Falls Sie die Möglichkeit haben, Ihre Anwesenheitszeiten bei der Regelfestlegung einzubeziehen, kann das Dienstprogramm Outbreak Manager die geeignete Reaktion, manuell oder automatisch, in Abhängigkeit von dem Zeitpunkt wählen, zu dem die Entdeckung stattfindet.

Je nach eingesetztem Virenschutzprogramm stehen eine oder mehrere der folgenden Aktionen für die Durchführung zur Verfügung:

- Löschen der infizierten E-Mail-Nachrichten
- Aktualisieren der .DAT-Dateien des Virenschutzprogramms
- Intensivieren der Viruserkennung
- Deaktivieren des Mail-Servers oder Virenschutzprogramms für einen bestimmten Zeitraum und Zurückweisen aller eingehenden E-Mail-Nachrichten

Das Dienstprogramm Outbreak Manager kennt auch Benachrichtigungen als Regelaktionen, so daß Sie über alle Aktivitäten im Zusammenhang mit Virusepidemien auf dem Laufenden gehalten werden.

Status und protokollierte Datensätze

Das Dienstprogramm ermöglicht es Ihnen, mit einem Mausklick den Status Ihrer Ausbruchregeln anzuzeigen. So können Sie den aktuellen Zustand der Regeln anzeigen und die jeweils zugeordneten Aktionen ausweiten, falls der Regelauslöser aktiviert wurde. Durch Kontrolle des Regelstatus sind Sie in der Lage zu beurteilen, mit welcher Genauigkeit Sie die Schwellenwerte der Regel festgelegt haben. Auf diese Weise können Sie die Regeln den besonderen Erfordernissen Ihrer Organisation anpassen.

Das Dienstprogramm protokolliert (standardmäßig) ständig den Status einer jeden Virusepidemie-Regel mit Hilfe des Dienstprogramms Log Manager, so daß Sie jederzeit (beispielsweise während einer Arbeitspause) den Status einer Regel und ihrer Aktivitäten im Zusammenhang mit Virusepidemien überprüfen können.

Zur Funktionsweise des Dienstprogramms Outbreak Manager

Microsoft Windows-Dienst

Das Dienstprogramm Outbreak Manager fungiert als Microsoft Windows-Dienst und ermöglicht Ihnen auf diese Weise eine kontinuierliche Überwachung Ihres Computers. Der Outbreak Manager-Dienst ist für folgendes verantwortlich:

- Test auf Virusepidemien unter Verwendung der von Ihnen konfigurierten Regeln.
- Versenden der Benachrichtigungen über Virusepidemien.
- Automatisches Durchführen der Aktionen bei Aktivierung des Regelauslösers bzw. gegebenenfalls Anzeigen einer Meldung, die zur Benutzerintervention auffordert.

Wenn Sie das Dienstprogramm Outbreak Manager öffnen und eine oder mehrere Virusausbruchregeln erstellen und anwenden, wird der Outbreak Manager-Dienst gestartet und am unteren Rand Ihres Bildschirms ein Outbreak Manager-Symbol angezeigt, das angibt, daß der Dienst ordnungsgemäß arbeitet.

Interaktion mit anderer Virenschutz-Software

Das Dienstprogramm Outbreak Manager kann mit den anderen verfügbaren McAfee-Virenschutzprogramm auf Ihrem Computer zusammenarbeiten. Welche der Auslöser, Reaktionen und Aktionen zur Verfügung stehen, hängt von den installierten Virenschutzprogrammen und den Leistungsmerkmalen ab, die Sie bei der Installation des Dienstprogramms Outbreak Manager gewählt haben.

Sie können mehr als eine Kopie von Outbreak Manager auf unterschiedlichen Computern aktivieren. Allerdings werden diese Kopien nicht miteinander kommunizieren.

Installieren, Aktualisieren und Entfernen des Dienstprogramms Outbreak Manager

Das Dienstprogramm Outbreak Manager kann bei der Installation Ihres Virenschutzprogramms installiert werden. Wenn Sie prüfen möchten, ob das Dienstprogramm Outbreak Manager ordnungsgemäß installiert wurde, überprüfen Sie das Outbreak Manager-Symbol in der Windows-Taskleiste.

Wenn Sie das Dienstprogramm Outbreak Manager vorher installiert haben, können Sie feststellen, welche Version der Software installiert wurde. Dazu klicken Sie mit der rechten Maustaste auf das Outbreak Manager-Symbol in der Windows-Taskleiste und wählen dann aus dem Kontextmenü die Option **Info**.

Das Installationsprogramm für Ihre Virenschutz-Software kann jederzeit zum Installieren oder Ändern des Dienstprogramms Outbreak Manager ausgeführt werden. Sie haben folgende Möglichkeiten:

- Installieren des Dienstprogramms Outbreak Manager, wenn es nicht zusammen mit Ihrem Virenschutzprogramm installiert wurde.
- Aktualisieren des Dienstprogramms Outbreak Manager mit neuen Funktionen für die neuen im Netzwerk ihres Unternehmens installierten Virenschutzprogramme.
- Reparieren der installierten Version des Dienstprogramms Outbreak Manager, wenn einige der Programmdateien oder Registrierungsdateien durch die Installation eines anderen Programms beschädigt wurden.
- Entfernen des Dienstprogramms Outbreak Manager.

Details zum Installieren Ihres Virenschutzprodukts finden Sie in Kapitel 2, „Erste Schritte.“.

Installationsanforderungen

McAfee empfiehlt, die folgenden Anforderungen vor dem Installieren des Dienstprogramms Outbreak Manager sorgfältig zu lesen, um sicherzustellen, daß die Installation problemlos verläuft und das Programm nahtlos integriert wird.

Rechte and Berechtigungen

Das Dienstprogramm Outbreak Manager wird unter Verwendung des Standardsystemkontos für Ihren Computer installiert. Sie benötigen *kein* Konto mit Administratorrechten. Wenn Sie jedoch das Dienstprogramm Outbreak Manager später aktualisieren, reparieren oder entfernen möchten, müssen Sie *dasselbe* Konto wie für die Installation verwenden.

Systemanforderungen

Das Dienstprogramm Outbreak Manager muß auf dem Computer installiert werden, auf dem Ihre Virenschutz-Software ausgeführt wird. Wenn dies nicht der Fall ist, kann das Dienstprogramm Outbreak Manager nicht mit der Virenschutz-Software zusammenarbeiten. Tabelle 11-1 auf Seite 227 zeigt die Systemanforderungen.

Tabelle 11-1. Systemanforderungen

	Mindestanforderung	Empfohlen
Prozessor	Intel Pentium-Prozessor, 133MHz MHz	Intel Pentium-Prozessor, 200 MHz
Hauptspeicher (Betriebssystem wählen):		
• Windows NT, Service Pack 4, 5 oder 6a	32 MB	64 MB
• Windows 2000 Server	128 MB	256 MB
• Windows 2000 Advanced Server	128 MB	256 MB
Freier Speicherplatz auf der Festplatte	160 MB	250 MB

Öffnen des Dienstprogramms Outbreak Manager

Sie können das Dienstprogramm Outbreak Manager folgendermaßen öffnen:

- Mit Hilfe des Windows-Menüs **Start** oder
- mit Hilfe des Outbreak Manager-Symbols in der Windows-Taskleiste.

  Das Outbreak Manager-Symbol wird angezeigt, wenn der Outbreak Manager-Dienst ordnungsgemäß läuft.

Zum Öffnen des Dienstprogramms Outbreak Manager führen Sie einen der folgenden Schritte durch:

1. Klicken Sie in Windows auf **Start** und zeigen Sie dann auf **Programme**.
2. Führen Sie einen der folgenden Schritte aus:

- suchen Sie nach der Programmgruppe Ihrer Virenschutz-Software oder der Programmgruppe **Network Associates** (abhängig davon, wo Sie das Dienstprogramm Outbreak Manager installiert haben) und klicken dann auf **Outbreak Manager**, oder

- klicken Sie mit der rechten Maustaste auf das Outbreak Manager-Symbol in der Windows-Taskleiste, und wählen Sie dann aus dem Kontextmenü die Option **Regeln konfigurieren**.

  Das Dialogfeld Outbreak Manager wird angezeigt (Abbildung 11-1 auf Seite 228).

Verwenden des Dienstprogramms Outbreak Manager

Das Dialogfeld Outbreak Manager (Abbildung 11-1) zeigt die Regeln, die vorher für die Erkennung und Behandlung von Virenepidemien festgelegt wurden. Wenn Sie keine Regeln angegeben haben, ist die angezeigte Liste leer. Beim Testen auf Virusepidemien arbeitet das Dienstprogramm die Regeln der Reihe nach von oben nach unten ab.

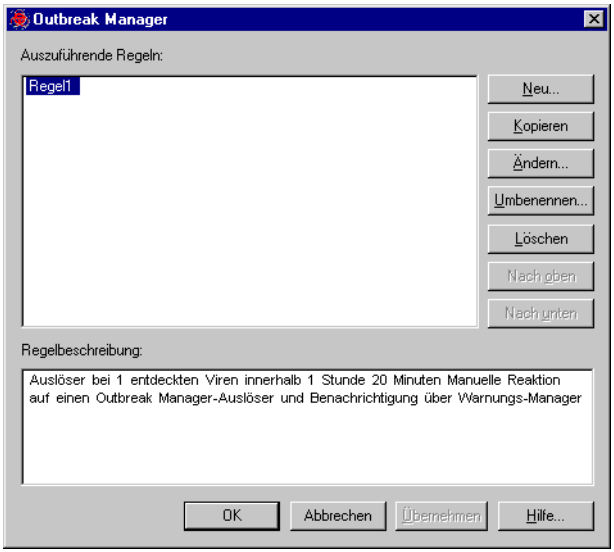


Abbildung 11-1 Dialogfeld „Outbreak Manager“

Wenn Sie in der Liste auf eine der Regeln klicken, erscheint eine Kurzbeschreibung der Auslöseparameter und Reaktionen aus dem Feld Regelbeschreibung.

Mit dem Dialogfeld Outbreak Manager haben Sie folgende Möglichkeiten:

- Erstellen neuer Regeln; siehe Seite 229.
- Ändern vorhandener Regeln; siehe Seite 239.
- Kopieren von Regeln; siehe Seite 240.

- Umbenennen von Regeln; siehe Seite 241.
- Löschen von Regeln; siehe Seite 242.
- Ändern der Reihenfolge von Regeln; siehe Seite 242.

Übernehmen Ihrer Änderungen

Wenn Sie Änderungen an den Einstellungen des Dienstprogramms Outbreak Manager vornehmen, müssen Sie diese Änderungen übernehmen, um die neuen Einstellungen zu speichern. Wenn Sie das Dialogfeld ohne Übernahme der Änderungen schließen, gehen diese verloren.

Verwenden Sie die Schaltflächen im Dialogfeld Outbreak Manager (Abbildung 11-1 auf Seite 228), um Ihre Änderungen zu übernehmen und das Dialogfeld zu schließen:

- **OK** übernimmt die Änderungen und schließt das Dialogfeld.
- **Abbrechen** schließt das Dialogfeld, ohne die Änderungen zu übernehmen.
- **Übernehmen** übernimmt die Änderungen, ohne das Dialogfeld zu schließen, damit Sie weitere Änderungen vornehmen können.

Wenn Sie Ihre Änderungen übernehmen, wird ein Meldungsfeld angezeigt, in dem Sie gefragt werden, ob Sie den Outbreak Manager-Dienst neu starten möchten. Wenn der Dienst neu gestartet wird, verwendet er zum Überprüfen, ob Virusepidemien vorliegen, Ihre neuen Einstellungen.

Erstellen neuer Regeln

Der Regelassistent führt Sie durch die einzelnen Konfigurationsschritte zur Erstellung einer neuen Regel. Eine Regel besteht hauptsächlich aus folgenden Komponenten:

- Auslöseparameter—Werte, deren Überschreitung das Dienstprogramm Outbreak Manager veranlassen, den Regelfall auszulösen und die zugeordneten Reaktionen und Aktionen durchzuführen.
- Reaktionen—Legen fest, wie das Dienstprogramm Outbreak Manager bei Regelauslösung (ohne Benutzerintervention) reagieren soll:
- Aktionen—Die Aktionen, die beim Auslösen der Regel durchgeführt werden. Wenn die Regel so konfiguriert ist, daß Benutzerintervention erforderlich ist, wird sie in einer Meldung angezeigt. Der Benutzer kann dann entscheiden, ob er die Aktion ausführt oder die Meldung ignoriert.

Welche der Auslöser, Reaktionen und Aktionen zur Verfügung stehen, hängt von den installierten Virenschutzprogrammen und den Leistungsmerkmalen ab, die Sie bei der Installation des Dienstprogramms Outbreak Manager gewählt haben.

Um eine neue Regel hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Dialogfeld Outbreak Manager. Genaue Informationen hierzu finden Sie unter “Öffnen des Dienstprogramms Outbreak Manager“ auf Seite 227.

2. Klicken Sie auf **Neu**.

   Der Regelassistent mit dem Fenster Regelauslöser (Abbildung 11-2 auf Seite 230) wird angezeigt. Hier können Sie den Auslöser für die Regel festlegen.

   Wählen Sie im Listenfeld Auslöser für diese Regel angeben die für die Regel erforderlichen Auslöser. Neben den Auslösern werden die verknüpften Virenschutzprogramme angezeigt, die die Auslöser überwachen.

Abbildung 11-2. Outbreak Manager-Assistent - Dialogfeld „Regelauslöser“

3. Wählen Sie im Feld Auslöser für diese Regel angeben den für die Regel erforderlichten Auslöser. Sie können nur einen Auslöser wählen.

   Die Beschreibung des gewählten Auslösers wird im Feld Auslöseparameter angezeigt. Hier können Sie auch die Werte des Auslösers angeben.

4. Legen Sie im Feld Auslöseparameter die erforderlichen Auslöseparameter fest.

   Die Parameter werden blau und unterstrichen angezeigt. Sofern ein Standardwert definiert ist, wird er angezeigt. Andernfalls erscheint ein Platzhaltertext, beispielsweise „Nummer von“.

TIP: Jede Organisation kennt jeweils andere Verfahrensweisen beim Erstellen neuer E-Mail-Nachrichten. Wenn Sie nicht sicher sind, welche Werte Sie. verwenden sollen, geben Sie für die Auslöseparameter hohe Werte an, und beobachten Sie den Status der Regel. Siehe unter "Anzeigen des Regelstatus" auf Seite 242. Sie werden bald ein Verständnis für den E-Mail-Durchsatz und den Grad des Virusbefalls Ihrer Organisation entwickeln und können dann die Regeln abändern, indem Sie die Auslöseparameter Ihren Erkenntnissen entsprechend anpassen.

So ändern Sie einen Parameter:

a. Klicken Sie auf den Wert oder Text des Parameters (er ist blau und unterstrichen). Dies ist vergleichbar mit einem HTML-Link auf einer Webseite.

   Es erscheint ein Dialogfeld, in dem Sie den gewünschten Wert angeben können.

b. Geben Sie unter Verwendung der Felder im Dialogfeld den gewünschten Wert an. Sind Schaltflächen mit Pfeilsymbolen („Nach oben" oder „Nach unten") vorhanden, können Sie den Wert unter Verwendung dieser Pfeile ändern.

c. Klicken Sie auf **OK**.

   Der angegebene Wert wird in die Beschreibung im Feld Auslöseparameter eingefügt.

5. Wenn alle Parameter festgelegt sind, klicken Sie auf **Weiter>**, um fortzufahren.

   Der Regelassistent zeigt das Dialogfeld Regelreaktionen (Abbildung 11-3) an. Hier können Sie die Reaktionen für die Regel festlegen.

Regel-Reaktionen
McAfee
Outbreak Manager
Geben Sie die Reaktion dieser Regel an:
Manuell reagieren
Automatisch reagieren
Benachrichtigung via Warnungs-Manager
Benachrichtigung via E-Mail-Nachricht
Geschäftszeiten verwenden
Reaktionsparameter (klicken Sie auf einen unterstrichenen Wert, um ihn zu bearbeiten):
Manuelle Reaktion auf einen Outbreak Manager-Auslöser und Benachrichtigung über Warnungs-Manager und sende E-Mail-Nachricht an E-Mail-Adresse (Server:25)
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 11-3. Outbreak Manager-Assistent - Dialogfeld „Regelreaktionen"

6. Wählen Sie aus, wie das Dienstprogramm Outbreak Manager bei Regelauslösung reagieren soll:

   - Wählen Sie **Manuell**, wenn das Dienstprogramm Outbreak Manager bei Regelauslösung eine Meldung anzeigen soll. Diese Variante erfordert die Intervention des Benutzers und ermöglicht es ihm, zwischen den möglichen Regelaktionen diejenige auszuwählen, die durchgeführt werden soll. Oder

   - Wählen Sie **Automatisch**, wenn das Dienstprogramm Outbreak Manager bei Regelauslösung die Aktionen der Regel automatisch durchführen soll, so daß keine Benutzerintervention erforderlich ist.

   Das Feld Reaktion für diese Regel angeben listet alle Reaktionen auf, die für diesen Reaktionstyp verfügbar sind.

7. Wählen Sie im Feld Reaktion für diese Regel angeben die erforderlichen Reaktionen aus.

   Aktivieren Sie dazu die Kontrollkästchen neben den gewünschten Reaktionen. Deaktivieren Sie die Kontrollkästchen neben den Reaktionen, die Sie *nicht* wünschen. Die Beschreibung der gewählten Reaktion erscheint im Feld „Reaktionsparameter“, in dem Sie auch die zugehörigen Werte angeben können.

   Je nach installiertem Virenschutzprogramm stehen eine oder mehrere der folgenden Reaktionen zur Verfügung:

   - Die Reaktion des Typs **Verwenden von Anwesenheitszeiten** (nur für *manuelle* Reaktionen) ermöglicht Ihnen, die Zeiten anzugeben, in denen Sie im Büro anwesend sind, so daß das Dienstprogramm Outbreak Manager während der restlichen Zeiten automatisch reagieren kann.

   - Die Reaktion des Typs **Benachrichtigung per E-Mail** veranlaßt das Dienstprogramm Outbreak Manager, Sie per E-Mail-Nachricht zu informieren. Bei automatischen Regeln wird die E-Mail-Nachricht erst gesendet, wenn *alle* Aktionen der Regel durchgeführt worden sind. Bei manuellen Regeln wird die E-Mail-Nachricht erst gesendet, wenn Sie die Bildschirmmeldung bestätigt haben, die alle fünf Minuten erscheint, nachdem *alle* Aktionen der Regel durchgeführt worden sind. Genaue Informationen zum Festlegen von Aktionen finden Sie unter Schritt 10 auf Seite 235.

- Die Reaktion des Typs **Benachrichtigung per Alert Manager** veranlaßt das Dienstprogramm Alert Manager, Sie unter Verwendung seiner Benachrichtigungsmethoden (beispielsweise E-Mail, Drucker, Pager oder Netzwerkmeldungen) zu alarmieren, wenn die Regel ausgelöst wird. Dazu muß das Dienstprogramm Alert Manager auf demselben Computer installiert sein und korrekt arbeiten, auf dem sich das Dienstprogramm Outbreak Manager befindet. Informationen zur Verwendung des Dienstprogramms Alert Manager finden Sie in Kapitel 8, „Viruswarnsystem.“.

8. Legen Sie im Feld Reaktionsparameter die erforderlichen Reaktionsparameter fest.

   Die Parameter werden blau und unterstrichen angezeigt. Sofern ein Standardwert definiert ist, wird er angezeigt. Andernfalls erscheint ein Platzhaltertext wie etwa „E-Mail-Adresse“.

   So ändern Sie einen Parameter:

   a. Klicken Sie auf den Wert oder Text des Parameters (er ist blau und unterstrichen).

      Es erscheint ein Dialogfeld, in dem Sie den gewünschten Wert angeben können.

   b. Geben Sie unter Verwendung der Felder im Dialogfeld den gewünschten Wert an. Sind Schaltflächen mit Pfeilsymbolen („Nach oben“ oder „Nach unten“) vorhanden, können Sie den Wert unter Verwendung dieser Pfeile ändern.

      Wenn Sie Anwesenheitszeiten festlegen, stellen die markierten Stundenblöcke (blau) die Stunden dar, in denen Sie im Büro sind. (Abbildung 11-4) Zur Auswahl eines Stundenblocks klicken Sie einmal darauf, um ihn blau einzufärben. Um die Auswahl eines Stundenblocks aufzuheben, klicken Sie erneut darauf, so daß der Block wieder weiß erscheint.

      Sie haben auch folgende Möglichkeiten:

      - Klicken Sie auf das graue Kästchen in der oberen linke Ecke des Rasters (oberhalb von „Montag“), um das gesamte Raster auszuwählen oder die Auswahl rückgängig zu machen.
      - Klicken Sie auf ein graues Kästchen für einen der Tage auf der linken Seite des Rasters, um alle Stunden eines Tags gleichzeitig auszuwählen oder die Auswahl rückgängig zu machen.
      - Klicken Sie auf ein graues Kästchen für eine Stunde am oberen Rand des Rasters, um die Stunde an allen Tagen auszuwählen oder die Auswahl rückgängig zu machen.

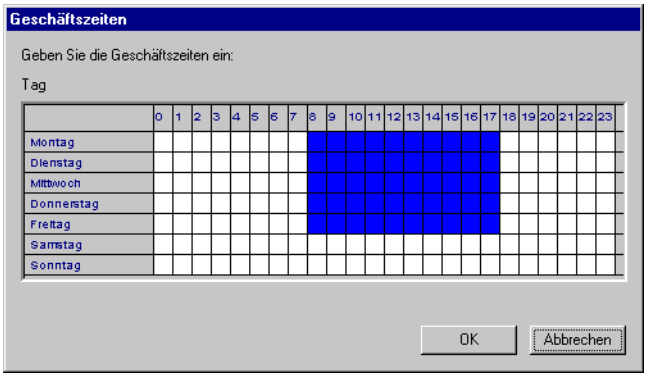


Abbildung 11-4. Dialogfeld „Anwesenheitszeiten“

c. Klicken Sie auf **OK**.

   Der angegebene Wert wird in die Beschreibung im Feld Reaktionsparameter eingefügt. Bei der Festlegung von Anwesenheitszeiten behält der Parametertext unverändert den Wert „Stunden“.

9. Wenn alle Parameter festgelegt sind, klicken Sie auf **Weiter>**, um fortzufahren.

   Der Regelassistent zeigt das Dialogfeld Regelaktionen (Abbildung 11-5) an. Hier können Sie die Aktionen für die Regel festlegen. Sie können mehrere Aktionen für eine Regel festlegen und diesen in der Liste Prioritäten zuweisen. Beim Auslösen der Regel wird das Dienstprogramm Outbreak Manager entweder

   - Die Aktionen in der Reihenfolge durchführen, die Sie festgelegt haben (sofern die Regel für eine automatische Reaktion ohne Benutzerintervention konfiguriert worden ist), oder
   - Diese Liste der Aktionen in einer Meldung präsentieren, so daß Sie die Möglichkeit haben, die durchzuführende Aktion auszuwählen. Dieser Fall tritt ein, wenn die Regel für eine manuelle Reaktion konfiguriert wurde, die eine Benutzerintervention erfordert.

Abbildung 11-5. Outbreak Manager-Assistent - Dialogfeld „Regelaktionen“

10. So fügen Sie eine Aktion für eine Regel hinzu:

    a. Klicken Sie auf **Hinzufügen**.

    Es erscheint das Dialogfeld Verfügbare Aktionen (Abbildung 11-6 auf Seite 236), in dem Sie die gewünschte Aktion festlegen können. Welche Aktionen zur Verfügung stehen, hängt davon ab:

    - welches Virenschutzprogramm installiert ist.
    - welche Funktionen während der Installation von Outbreak Manager installiert wurden.

    Die Priorität der Aktion gibt an, wie schwerwiegend die Konsequenzen sind. 1 charakterisiert diejenigen mit höchster Priorität, beispielsweise das Herunterfahren des MailScan-Dienstes. 5 charakterisiert diejenigen mit niedrigster Priorität, beispielsweise das Ausführen einer DAT-Aktualisierung.

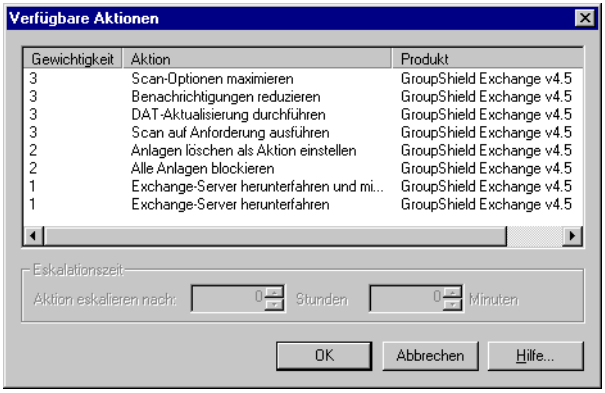


Abbildung 11-6. Dialogfeld „Verfügbare Aktionen“

b. Wählen Sie die erforderliche Aktion im Listenfeld aus.

c. Wenn die Konfiguration der Regel eine automatische Reaktion vorsieht, müssen Sie im Feld Ausweitungszeitraum einen Ausweitungszeitraum angeben. Die Zeitangabe muß mindestens 1 Minute betragen.

   Der Ausweitungszeitraum definiert den Punkt, ab dem Outbreak Manager mit der Durchführung der Aktion beginnt, sofern die Bedingungen für die Regelauslösung nach Ablauf der angegebenen Zeit im Anschluß an die erstmalige Regelauslösung immer noch zutreffen.

   Wenn Sie beispielsweise für eine Aktion einen Ausweitungszeitraum von 30 Minuten angeben, wird die Aktion nicht durchgeführt, falls innerhalb der ersten 30 Minuten nach erstmaliger Auslösung die Regel erneut ausgelöst wird. Sollte die Regel nach Ablauf der 30 Minuten weiterhin ausgelöst werden, wird die Aktion durchgeführt.

TIP: Die Funktion des Ausweitungszeitraums ermöglicht die Definition sehr flexibler Regeln, die die Prioritäten ihrer Aktionen mit der Zeit anheben, wenn die Regel kontinuierlich neu ausgelöst wird. Sie können beispielsweise eine Regel konfigurieren, welche im Anfangsstadium die Aktualisierung der .DAT-Dateien des Virenschutzprogramms veranlaßt und schließlich (als letzte drastische Maßnahme) den Mail-Server herunterfährt, wenn die Bedingungen für die Virusepidemie nach einer gewissen Zeitspanne immer noch diagnostiziert werden.

---

d. Klicken Sie auf **OK**.

Wenn die Aktion eine Priorität von 1 hat, erscheint eine Meldung, um Sie an die Wichtigkeit der Aktion zu erinnern. Klicken Sie dann zur Bestätigung auf **OK**.

Die Aktion wird zu der im Dialogfeld Regelaktionen angezeigten Liste hinzugefügt (Abbildung 11-5 auf Seite 235).

11. Um eine Aktion zu entfernen, markieren Sie sie in der Liste und klicken dann auf **Entfernen**.

12. Soll die Reihenfolge geändert werden, in der die Aktionen durchgeführt werden, so können Sie die Schaltflächen **Nach oben** und **Nach unten** verwenden, um die Aktionen in der Aktionsliste zu verschieben.

    Um eine Aktion zu verschieben, markieren Sie die Aktion, die Sie verschieben möchten, und verwenden dann die Schaltflächen **Nach oben** und **Nach unten**, um die Aktion an die gewünschte Position innerhalb der Liste zu verschieben.

13. Standardmäßig wird der Status der Regel durch das Dienstprogramm Log Manager erfaßt. So können Sie die Werte anzeigen, die zum Auslösen der Regel geführt haben, sowie Angaben über die Aktionen, die durchgeführt worden sind. Informationen zur Verwendung des Dienstprogramms Log Manager finden Sie auf Seite 244.

    Wenn Sie den Status einer Regel nicht protokollieren möchten, müssen Sie das Kontrollkästchen **Umfassende Protokollierung für diese Regel aktivieren** deaktivieren.

14. Wenn Sie die Festlegung der Aktionen für die Regel beendet und die Aktionen in der erforderlichen Weise mit Prioritäten versehen haben, klicken Sie auf **Weiter>**, um fortzufahren.

    Der Regelassistent zeigt das Dialogfeld Regelübersicht an (Abbildung 11-7).

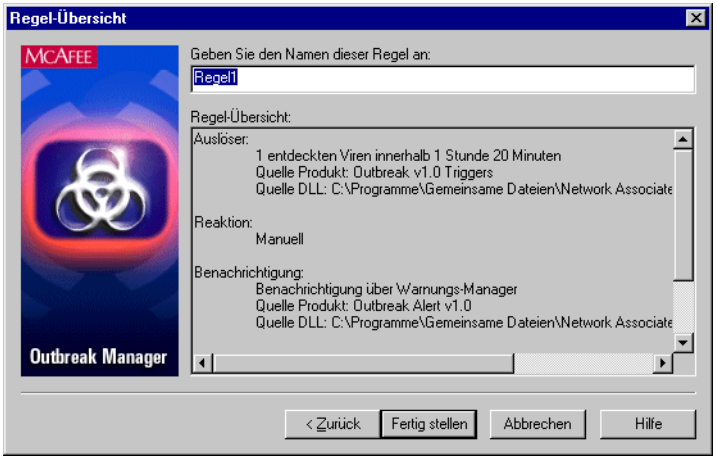


Abbildung 11-7. Outbreak Manager-Assistent - Dialogfeld „Regelübersicht“

15. Geben Sie einen Namen für die Regel in das Textfeld ein.

    Der Regelname erscheint in der Liste der Regeln im Dialogfeld Outbreak Manager (Abbildung 11-1 auf Seite 228). Versuchen Sie, eine kurze Beschreibung der Regeleinstellungen in den neu vergebenen Namen einfließen zu lassen, so daß Sie die Regel leichter in der Liste finden können.

    ❑ **ANMERKUNG:** Regelnamen müssen eindeutig sein. Sie müssen also einen Namen eingeben, der noch nicht für eine andere Regel verwendet wird.

16. Überprüfen Sie Ihre Einstellungen für die Regel im Feld Regelübersicht. Anschließend haben Sie zwei Möglichkeiten:

    - Entweder Sie ändern die Einstellungen, indem Sie auf die Schaltfläche **<Zurück** klicken, um zu den vorhergehenden Fenstern des Regelassistenten zurückzukehren, oder
    - Sie bestätigen die Einstellungen, indem Sie auf **Fertigstellen** klicken.

      Die Virusepidemie-Regel wurde damit zum Dienstprogramm Outbreak Manager hinzugefügt.

17. Übernehmen Sie Ihre Änderungen, und starten Sie den Outbreak Manager-Dienst neu. Genaue Informationen hierzu finden Sie unter “Übernehmen Ihrer Änderungen“ auf Seite 229.

Sie haben folgende Möglichkeiten:

- Informationen zum Ändern der Position der neuen Regel innerhalb der Regelliste finden Sie unter “Ändern der Reihenfolge von Regeln“ auf Seite 242.
- Informationen zum Duplizieren der neuen Regel, um schnell eine ähnliche Regel zu erstellen, finden Sie unter “Kopieren von Regeln“ auf Seite 240.

Ändern vorhandener Regeln

Durch Modifizieren einer Virusepidemie-Regel können Sie die Einstellungen für die Erkennung des Epidemieausbruchs und die Reaktionen auf einen solchen Ausbruch ändern. Sie haben folgende Möglichkeiten:

- Optimieren der Regelschwellenwerte durch größere oder kleinere Werte für die Auslöseparameter oder
- Ändern der Reaktionsweise der Regel oder
- Ändern der Aktionen, die beim Auslösen der Regel durchgeführt oder zur Durchführung vorgeschlagen werden.

Zum Ändern einer Regel führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Dialogfeld Outbreak Manager. Genaue Informationen hierzu finden Sie unter “Öffnen des Dienstprogramms Outbreak Manager“ auf Seite 227.
2. Wählen Sie in der Regelliste die Regel aus, die Sie ändern möchten.
3. Klicken Sie auf **Ändern**.

   Der Regelassistent zeigt das Dialogfeld Regelauslöser an (Abbildung 11-2 auf Seite 230). Die Felder im Regelassistenten enthalten die aktuellen Einstellungen für die Regel, die Sie gerade ändern.
4. Fahren Sie fort mit Schritt 3 auf Seite 230 bis Schritt 17.

Löschen von Regeln

Das Löschen einer Virusepidemie-Regel entfernt die Regel endgültig aus dem Dienstprogramm Outbreak Manager. Soll die Regel mit geänderten Einstellungen erhalten bleiben, können Sie sie zu diesem Zweck ändern. Informationen finden Sie unter “Ändern vorhandener Regeln” weiter oben.

To delete a rule, follow these steps:

1. Open the Outbreak Manager dialog box. For details on doing this, see “Öffnen des Dienstprogramms Outbreak Manager“ auf Seite 227.
2. Wählen Sie in der Regelliste die Regel aus, die Sie löschen möchten.
3. Klicken Sie auf **Löschen**.

   Die Virusepidemie-Regel wurde aus dem Dienstprogramm Outbreak Manager entfernt.
4. Übernehmen Sie Ihre Änderungen, und starten Sie den Outbreak Manager-Dienst neu. Genaue Informationen hierzu finden Sie unter “Übernehmen Ihrer Änderungen“ auf Seite 229.

Kopieren von Regeln

Das Kopieren einer Virusepidemie-Regel erstellt eine neue Regel mit identischen Einstellungen (ein Duplikat). Anschließend können Sie die neue Regel ändern.

TIP: Mit dieser Funktion können Sie schnell und problemlos eine Regel mit ähnlichen Einstellungen wie denen einer bereits vorhandenen Regel erstellen. Dazu kopieren Sie einfach die vorhandene Regel und bearbeiten anschließend die Kopie in der erforderlichen Weise. Siehe unter “Ändern vorhandener Regeln“ auf Seite 239.

Zum Kopieren einer Regel, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Dialogfeld Outbreak Manager. Genaue Informationen hierzu finden Sie unter “Öffnen des Dienstprogramms Outbreak Manager“ auf Seite 227.
2. Wählen Sie in der Regelliste die Regel aus, die Sie kopieren möchten.
3. Klicken Sie auf **Kopieren**.

   Es erscheint das Dialogfeld Kopieren, in dem Sie einen Namen für die Kopie angeben können.
4. Geben Sie einen Namen für die Regel in das Textfeld ein.

   Der Regelname erscheint in der Liste der Regeln im Dialogfeld Outbreak Manager (Abbildung 11-1 auf Seite 228). Versuchen Sie, eine kurze Beschreibung der Regeleinstellungen in den neu vergebenen Namen einfließen zu lassen, so daß Sie die Regel leichter in der Liste finden können.

❒ **ANMERKUNG:** Regelnamen müssen eindeutig sein. Sie müssen also einen Namen eingeben, der noch nicht für eine andere Regel verwendet wird.

5. Klicken Sie auf **OK**.

   Sie haben eine Regel mit duplizierten Einstellungen und dem von Ihnen eingegebenen Namen erstellt.

   Informationen zum Ändern der neuen Regel finden Sie unter “Ändern vorhandener Regeln“ auf Seite 239.

6. Übernehmen Sie Ihre Änderungen, und starten Sie den Outbreak Manager-Dienst neu. Genaue Informationen hierzu finden Sie unter “Übernehmen Ihrer Änderungen“ auf Seite 229.

Umbenennen von Regeln

Mit der Umbenennung einer Virusepidemie-Regel haben Sie die Möglichkeit, ihr einen aussagekräftigeren Namen zuzuordnen, um auf diese Weise die Regel leichter in der Regelliste finden zu können.

Zum Umbenennen einer Regel führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Dialogfeld Outbreak Manager. Genaue Informationen hierzu finden Sie unter “Öffnen des Dienstprogramms Outbreak Manager“ auf Seite 227.
2. Wählen Sie in der Regelliste die Regel aus, die Sie umbenennen möchten.
3. Klicken Sie auf **Umbenennen**.

   Es erscheint das Dialogfeld Umbenennen.

4. Geben Sie den erforderlichen Namen in das Textfeld ein.

   Der Regelname erscheint in der Liste der Regeln im Dialogfeld Outbreak Manager (Abbildung 11-1 auf Seite 228), verwenden Sie daher möglichst einen Namen, der die Einstellungen der Regel kurz beschreibt.

❒ **ANMERKUNG:** Regelnamen müssen eindeutig sein. Sie müssen also einen Namen eingeben, der noch nicht für eine andere Regel verwendet wird.

5. Klicken Sie auf **OK**.

   Die Regel wurde umbenannt.

6. Übernehmen Sie Ihre Änderungen, und starten Sie den Outbreak Manager-Dienst neu. Genaue Informationen hierzu finden Sie unter “Übernehmen Ihrer Änderungen“ auf Seite 229.

Ändern der Reihenfolge von Regeln

Bei der Suche nach Virusepidemien arbeitet das Dienstprogramm Outbreak Manager die Virusepidemie-Regeln in der Reihenfolge ab, in der sie in der Regelliste aufgeführt sind. Es kann vorkommen, daß Sie die Reihenfolge der Regeln ändern möchten, um die wichtigeren Regeln an den Anfang der Liste zu stellen und ihnen auf diese Weise eine höhere Priorität zuzuweisen.

Werden die in den Auslöseparametern einer Regel festgelegten Schwellenwerte überschritten, zeigt dies definitionsgemäß eine Virusepidemie an, und die Regel wird ausgelöst. Sie reagiert in der von Ihnen konfigurierten Weise, indem sie die verschiedenen Aktionen, die Sie für die Regel festgelegt haben, entweder direkt durchführt oder zur Durchführung vorschlägt.

Zum Ändern der Position einer Regel innerhalb der Regelliste führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Dialogfeld Outbreak Manager. Genaue Informationen hierzu finden Sie unter “Öffnen des Dienstprogramms Outbreak Manager“ auf Seite 227.
2. Wählen Sie in der Regelliste die Regel aus, die Sie verschieben möchten.
3. Verwenden Sie die Schaltflächen **Nach oben** und **Nach unten**, um die Regel an die gewünschte Position innerhalb der Liste zu verschieben.

   Um die Regel nach oben zu verschieben und auf diese Weise ihre Priorität zu erhöhen, klicken Sie auf **Nach oben**. Um die Regel nach unten zu verschieben und auf diese Weise ihre Priorität zu verringern, klicken Sie auf **Nach unten**.
4. Übernehmen Sie Ihre Änderungen, und starten Sie den Outbreak Manager-Dienst neu. Genaue Informationen hierzu finden Sie unter “Übernehmen Ihrer Änderungen“ auf Seite 229.

Anzeigen des Regelstatus

Sie können jederzeit den Zustand Ihrer Regeln überprüfen und die Zählerwerte der zugehörigen Regelauslöser der Regeln anzeigen. Wenn eine Regel ausgelöst wurde, können Sie die durchgeführte Aktion auch rückgängig machen.

Wenn Sie den E-Mail-Durchsatz und den Grad des Virusbefalls Ihrer Organisation nicht genau kennen, hilft Ihnen diese Funktion bei der Überwachung dieser Größen. Auf diese Weise können Sie die Größenordnung des Phänomens besser einschätzen und Ihre Regelauslöser dementsprechend anpassen.

Zum Anzeigen des Status einer Regel führen Sie die folgenden Schritte aus:

1. Klicken Sie mit der rechten Maustaste auf das Outbreak Manager-Symbol im Windows-Systemfeld.

   Es erscheint ein Kontextmenü.

2. Zeigen Sie auf **Regelstatus anzeigen**.

   Es erscheint ein Untermenü (Abbildung 11-8), in dem die Regeln aufgelistet sind, die Sie konfiguriert haben.

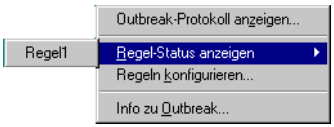


Abbildung 11-8. Untermenü „Regelstatus anzeigen“

3. Wählen Sie im Menü die gewünschte Regel.

   Es erscheint das Dialogfeld Outbreak Manager Trigger Plugin mit den aktuellen Statusinformationen der Regel. Wenn die Schwellenwerte der Regel überschritten wurden (Abbildung 11-9), ermöglicht Ihnen dieses Dialogfeld:

   - alle Aktionen rückgängig zu machen, die infolge der Regelauslösung durchgeführt worden sind. Diesen Zweck erreichen Sie durch Auswahl der Option **Alle Aktionen rückgängig**.
   - die Regel auf ihre nächste Aktion auszuweiten. Dazu wählen Sie die Option **Aktionen ausweiten**.

     Beim Erstellen einer Regel konfigurieren Sie für die verschiedenen Aktionen sogenannte Ausweitungszeiten, die festlegen, daß die Aktionen nur dann durchzuführen sind, wenn die Regel nach dem Ablauf der durch den Ausweitungszeitraum definierten Periode weiterhin Virusepidemien feststellt. Dieses Funktionsmerkmal veranlaßt die Regel, zur nächsten Aktion überzugehen, um diese durchzuführen.

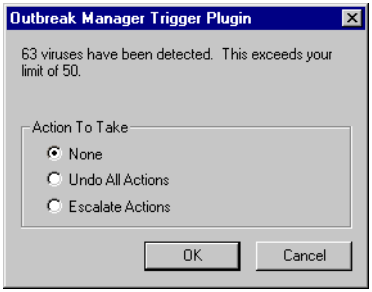


Abbildung 11-9. Dialogfeld „Outbreak Manager Trigger Plugin“ Überschrittene Schwellenwerte

4. Klicken Sie auf **OK**.

Anzeigen des Ausbruchaktivität

Das Dienstprogramm Outbreak Manager umfaßt ein Dienstprogramm namens Log Manager, das Ereignisse aufzeichnet, die in Outbreak Manager auftreten, beispielsweise die von ihm durchgeführten Aktionen und die von ihm registrierten Virusausbruch-Aktivitäten. Mit dem Dienstprogramm Log Manager können Sie nachvollziehen, was geschehen ist und nach bestimmten Arten von Ereignissen filtern.

Um das Dienstprogramm Log Manager zu öffnen, führen Sie die folgenden Schritte aus:

1. Klicken Sie mit der rechten Maustaste auf das Outbreak Manager-Symbol im Windows-Systemfeld.

   Es erscheint ein Kontextmenü.

2. Wählen Sie im Kontextmenü den Befehl **Ausbruchsprotokoll anzeigen**.

   Das Dienstprogramm Log Manager wird angezeigt (Abbildung 11-10).

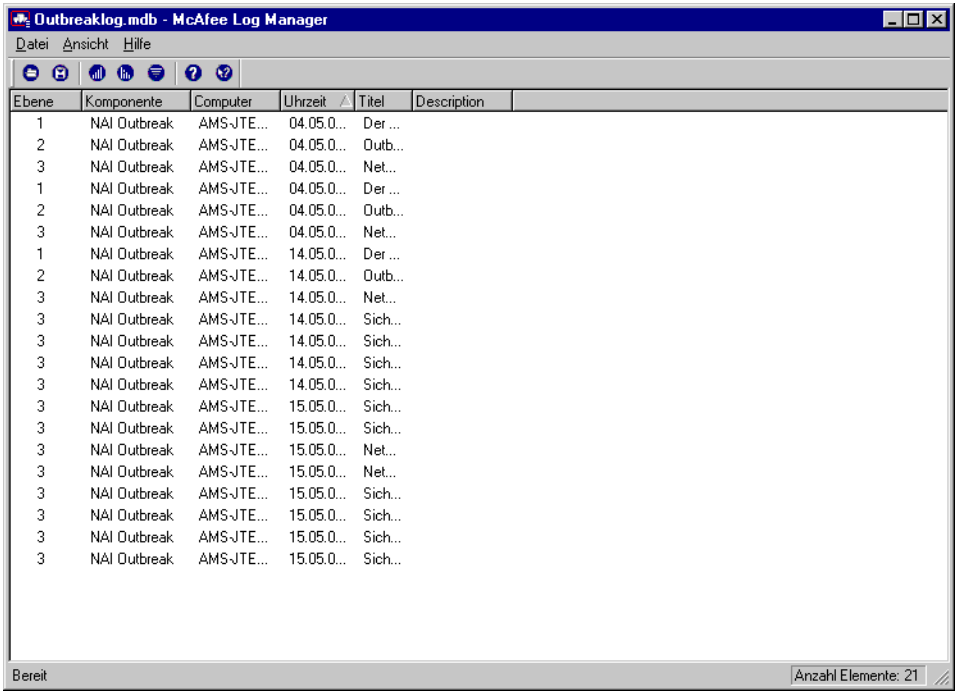

Outbreaklog.mdb - McAfee Log Manager
Datei Ansicht Hilfe
Ebene Komponente Computer Uhrzeit Titel Description
1 NAI Outbreak AMS-JTE... 04.05.0... Der ...
2 NAI Outbreak AMS-JTE... 04.05.0... Outb...
3 NAI Outbreak AMS-JTE... 04.05.0... Net...
1 NAI Outbreak AMS-JTE... 04.05.0... Der ...
2 NAI Outbreak AMS-JTE... 04.05.0... Outb...
3 NAI Outbreak AMS-JTE... 04.05.0... Net...
1 NAI Outbreak AMS-JTE... 14.05.0... Der ...
2 NAI Outbreak AMS-JTE... 14.05.0... Outb...
3 NAI Outbreak AMS-JTE... 14.05.0... Net...
3 NAI Outbreak AMS-JTE... 14.05.0... Sich...
3 NAI Outbreak AMS-JTE... 14.05.0... Sich...
3 NAI Outbreak AMS-JTE... 14.05.0... Sich...
3 NAI Outbreak AMS-JTE... 14.05.0... Sich...
3 NAI Outbreak AMS-JTE... 15.05.0... Sich...
3 NAI Outbreak AMS-JTE... 15.05.0... Sich...
3 NAI Outbreak AMS-JTE... 15.05.0... Net...
3 NAI Outbreak AMS-JTE... 15.05.0... Net...
3 NAI Outbreak AMS-JTE... 15.05.0... Sich...
3 NAI Outbreak AMS-JTE... 15.05.0... Sich...
3 NAI Outbreak AMS-JTE... 15.05.0... Sich...
3 NAI Outbreak AMS-JTE... 15.05.0... Sich...
Bereit
Anzahl Elemente: 21

Abbildung 11-10. Dienstprogramm Log Manager

Das Dienstprogramm Log Manager stellt Informationen zu Systemereignissen und Ausbruchaktivitäten bereit, die in seiner Datenbank gespeichert werden. Das Dienstprogramm besteht aus drei verschiedenen Bereichen zur Konfiguration und Informationsanzeige:

- Menüleiste
- Symbolleiste
- Ergebnisfenster

Sie können alle Datensätze in der Log Manager-Datenbank anzeigen oder Datensätze filtern, um eine bestimmte Untergruppe der Datensätze anzuzeigen. Informationen zum Filtern der Log Manager-Datenbank finden Sie auf Seite 248.

Menüleiste

Verwenden Sie die Menüleiste, um das Dienstprogramm Log Manager zu konfigurieren und Informationen über die einzelnen aufgezeichneten Ereignisse anzuzeigen.

Menü „Datei“

Das Menü **Datei** enthält die folgenden Befehle:

- Mit **Öffnen** wird eine zuvor gespeicherte Log Manager-Datenbank oder eine Datenbank auf einem anderen Server geöffnet.
- Mit **Speichern unter** wird die *aktuelle* Ansicht von Log Manager zu Analyse- oder Archivierungszwecken unter einem anderen Dateinamen abgelegt. Wenn Sie einen Filter angewendet haben, wird die angezeigte Untergruppe der Datensätze gespeichert. Die im .CSV-Format gespeicherte Datei kann in Microsoft Excel importiert werden, um dort analysiert und ausgewertet zu werden.
- Mit **Gefilterte Datensätze löschen** werden *gefilterte* Datensätze aus der Log Manager-Datenbank entfernt. Wenn Sie einen Filter angewendet haben, wird die angezeigte Untergruppe der Datensätze permanent entfernt. Diese Aktion kann *nicht* rückgängig gemacht werden.
- Mit **Gesamtes Protokoll löschen** werden *alle* Datensätze aus der Log Manager-Datenbank entfernt. Diese Aktion kann *nicht* rückgängig gemacht werden.
- Mit **Beenden** wird das Dienstprogramm Log Manager geschlossen.

Menü „Ansicht“

Das Menü **Ansicht** enthält die folgenden Befehle:

- Mit **Aktualisieren** wird die aktuelle Ansicht der Log Manager-Datenbank mit Datensätzen aktualisiert, die seit dem Öffnen des Dienstprogramms protokolliert wurden.
- **Filtern** erlaubt das Erstellen, Ändern oder Löschen von Filtern. Mit Hilfe von Filtern können Untergruppen von Datensätzen aus der Log Manager-Datenbank angezeigt werden. Informationen zum Filtern der Log Manager-Datenbank finden Sie auf Seite 248.
- **Spalten** dient der Festlegung, welche der Spalten im Ergebnisfenster sichtbar sein sollen.
- **Details** zeigt Informationen zu dem im Ergebnisfenster ausgewählten Datensatz an.

Der untere Teil des Menüs **Ansicht** zeigt Log Manager-Komponenten an. Diese können hier aus- oder eingeblendet werden.

Menü „Hilfe“

Das Menü **Hilfe** enthält die folgenden Befehle:

- Mit **Hilfethemen** wird das Online-Hilfesystem für Log Manager geöffnet. Mit den Befehlen Inhalt, Index und Suchen können Sie nach den gewünschten Informationen suchen.
- **Info** zeigt Copyright- und Systeminformationen für das Dienstprogramm an.

Symbolleiste

Verwenden Sie die Symbolleiste, um die Ansicht für Log Manager festzulegen, Copyright-Informationen anzuzeigen und das Online-Hilfesystem für Log Manager anzuzeigen. Die folgenden Symbole stehen zur Verfügung:

Öffnet eine zuvor gespeicherte Log Manager-Datenbank oder eine Datenbank auf einem anderen Server.

Hiermit wird die *aktuelle* Ansicht von Log Manager zu Analyse- oder Archivierungszwecken unter einem anderen Dateinamen abgelegt. Wenn Sie einen Filter angewendet haben, wird die angezeigte Untergruppe der Datensätze gespeichert. Die im .CSV-Format gespeicherte Datei kann in Microsoft Excel importiert werden, um dort analysiert und ausgewertet zu werden.

Sortiert die Datensätze in aufsteigender Reihenfolge, basierend auf den Einträgen in der ausgewählten Spalte. Zum Auswählen einer Spalte klicken Sie auf den Spaltenkopf.

Sortiert die Datensätze in absteigender Reihenfolge, basierend auf den Einträgen in der ausgewählten Spalte. Zum Auswählen einer Spalte klicken Sie auf den Spaltenkopf.

Erlaubt das Erstellen, Ändern oder Löschen von Filtern. Mit Hilfe von Filtern können Untergruppen von Datensätzen aus der Log Manager-Datenbank angezeigt werden. Informationen zum Filtern der Log Manager-Datenbank finden Sie auf Seite 248.

Zeigt Copyright- und Systeminformationen für das Dienstprogramm an.

Zeigt die Direkthilfe zu einem Element auf dem Bildschirm an. Klicken Sie auf das Symbol und dann auf das Bildschirmelement, zu dem Sie Informationen anzeigen möchten.

Ergebnisfenster

Das Ergebnisfenster zeigt die folgenden Spalten mit Informationen zu den angezeigten Ereignisdatensätzen an:

- **Grad** zeigt die Wichtigkeit des protokollierten Ereignisses an. 1 ist ein Warnereignis (höchster Schweregrad) für Ereignisse wie z. B. das Fehlschlagen einer Aufgabe des Outbreak Manager-Dienstes. 3 ist ein Informationsereignis (geringster Schweregrad) für Ereignisse wie z. B. den Status einer Ausbruchregel.
- **Komponente** verweist auf das Systemobjekt, welches das Ereignis verursacht hat. Für das Dienstprogramm Outbreak Manager wird „NAI Outbreak“ angezeigt.
- **Computer** gibt den Namen des Computers an, auf dem das Ereignis stattfand.
- **Zeitpunkt** gibt den Zeitpunkt an, an dem das Ereignis stattfand.
- **Titel** gibt an, welches Systemereignis oder Virusereignis stattgefunden hat.
- **Bezeichnung** beschreibt die Aktion, die als Reaktion auf das Ereignis durchgeführt wurde.

Verwenden Sie das Menü **Ansicht**, um den Typ der im Ergebnisfenster sichtbaren Informationen zu ändern.

Durch Klicken mit der rechten Maustaste auf Spaltenüberschriften können Sie Konfigurationsoptionen für die Spalten anzeigen. In rot dargestellte Spaltenüberschriften, die mit dem Symbol gekennzeichnet sind, zeigen an, daß für diese Spalte ein aktiver Filter existiert, der bewirkt, daß im Ergebnisfenster eine Untergruppe der Datensätze aus der Log Manager-Datenbank angezeigt wird.

Zum Auswählen eines Datensatzes im Ergebnisfenster klicken Sie auf den betreffenden Eintrag in der Spalte Grad.

Filtern der Log Manager-Datenbank

Sie können für das Dienstprogramm Log Manager auch Filter erstellen, um Untergruppen von Datensätzen aus der Log Manager-Datenbank anzuzeigen. Angezeigte gefilterte Datensätze können in einer Datei gespeichert werden, um analysiert, archiviert oder gelöscht zu werden, wenn sie nicht mehr benötigt werden.

Filter können für die Spalten im Ergebnisfenster erstellt werden. Sie können mehrere Filter erstellen, für eine oder mehrere Spalten, um genau die von Ihnen gewünschte Untergruppe von Datensätzen anzuzeigen.

ANMERKUNG: Wenn das Dienstprogramm Log Manager geschlossen wird, gehen alle Filter verloren.

Um einen neuen Filter zu erstellen, führen Sie die folgenden Schritte aus:

1. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf , oder
   - Wählen Sie die Option **Filter** aus dem Menü **Ansicht**.

   Das Dialogfeld Filterabfrage wird angezeigt (Abbildung 11-11). Es zeigt die derzeit verwendeten Filter an.

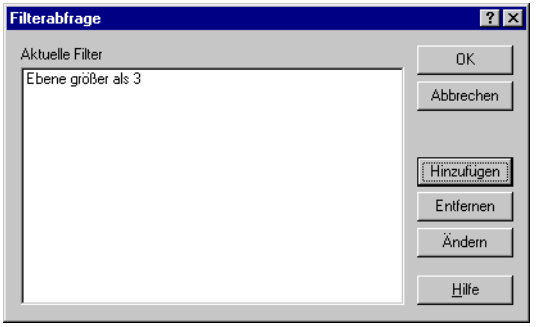


Abbildung 11-11. Dialogfeld „Filterabfrage“

2. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld Filterspalte wird angezeigt (Abbildung 11-12).

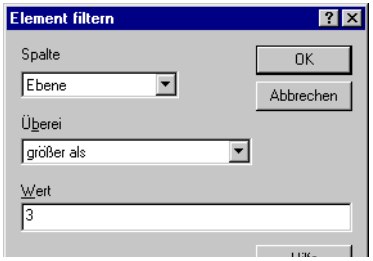


Abbildung 11-12. Dialogfeld „Filterspalte“

3. Legen Sie im Dialogfeld Spalte fest, nach welcher Spalte im Ergebnisfenster gefiltert werden soll.
4. Legen Sie im Kombinationsfeld Übereinstimmungen die Auswahlkriterien für den Filter fest.
5. Geben Sie den erforderlichen Wert in das Textfeld ein.
6. Klicken Sie auf **OK**.

   Der Filter wird im Dialogfeld Filterabfrage angezeigt.

7. Um weitere Filter zu erstellen, wiederholen Sie für jeden Filter Schritt 2 bis Schritt 6.

8. Wenn Sie die Filtererstellung abgeschlossen haben, klicken Sie im Dialogfeld Filterabfrage auf **OK**.

   Das Ergebnisfenster zeigt jetzt die Datensätze an, die Ihren Filterkriterien entsprechen. Die Überschriften der gefilterten Spalten sind in rot dargestellt und mit dem Symbol gekennzeichnet.

Zum Ändern eines Filters führen Sie die folgenden Schritte aus:

1. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf , oder
   - Wählen Sie die Option **Filter** aus dem Menü **Ansicht**.

   Das Dialogfeld Filterabfrage wird angezeigt (Abbildung 11-11 auf Seite 249). Es zeigt die derzeit verwendeten Filter an.

2. Wählen Sie den Filter aus, den Sie ändern möchten, und klicken Sie dann auf **Ändern**.

   Das Dialogfeld Filterspalte wird angezeigt (Abbildung 11-12 auf Seite 249). Es enthält die Filtereinstellungen.

3. Legen Sie im Kombinationsfeld Übereinstimmungen die Auswahlkriterien für den Filter fest.

4. Geben Sie den erforderlichen Wert in das Textfeld ein.

5. Klicken Sie auf **OK**.

   Der Filter wird im Dialogfeld Filterabfrage angezeigt.

6. Klicken Sie im Dialogfeld Filterabfrage auf **OK**.

   Das Ergebnisfenster zeigt jetzt die Datensätze an, die Ihren Filterkriterien entsprechen.

Zum Entfernen aller Filter für eine Spalte führen Sie die folgenden Schritte aus:

1. Klicken Sie mit der rechten Maustaste im Ergebnisfenster auf die Spaltenüberschrift der Spalte, deren Filter Sie entfernen möchten.

   Es erscheint ein Kontextmenü.

2. Wählen Sie im Kontextmenü den Befehl **Filter entfernen**.

Die Filter der Spalte werden entfernt. Das Ergebnisfenster zeigt jetzt die Datensätze an, die allen noch aktiven Filterkriterien entsprechen.

Anzeigen von Informationen zu einem Datensatz

Zum Anzeigen von Informationen für einen Datensatz führen Sie die folgenden Schritte aus:

1. Zum Auswählen eines Datensatzes im Ergebnisfenster klicken Sie auf den betreffenden Eintrag in der Spalte Grad.
2. Wählen Sie die Option **Details** aus dem Menü **Ansicht**.

   Das Dialogfeld Datensatzdetails wird angezeigt (Abbildung 11-13). Es enthält Informationen zum Datensatz.

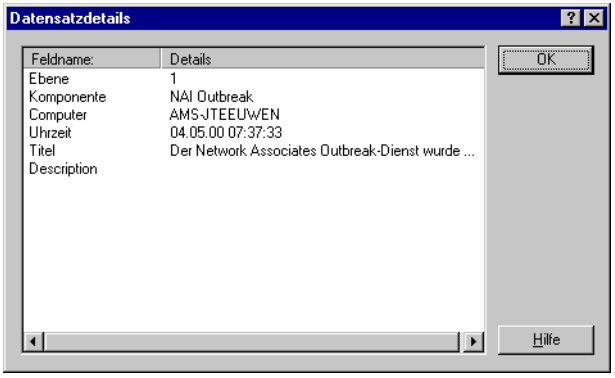


Abbildung 11-13. Dialogfeld „Datensatzdetails“

3. Wenn Sie die Informationen angesehen haben, klicken Sie auf **OK**.

Speichern von Datensätzen

Sie können die *aktuelle* Ansicht der Log Manager-Datenbank (im Ergebnisfenster) zu Analyse- oder Archivierungszwecken unter einem anderen Dateinamen speichern. Wenn Sie einen Filter angewendet haben, wird die angezeigte Untergruppe der Datensätze gespeichert. Die im .CSV-Format gespeicherte Datei kann in Microsoft Excel importiert werden, um dort analysiert und ausgewertet zu werden. Informationen zum Filtern der Log Manager-Datenbank finden Sie auf Seite 248.

Zum Speichern der Informationen in der Anzeige führen Sie die folgenden Schritte aus:

1. Wählen Sie aus dem Menü **Datei** den Befehl Speichern unter.

   Das Dialogfeld Speichern unter wird angezeigt (Abbildung 11-13). Es enthält Informationen zum Datensatz.

2. Geben Sie den Dateinamen und das Verzeichnis an, und klicken Sie auf **Speichern**.

Entfernen von Datensätzen

Sie haben folgende Möglichkeiten:

- Entfernen Sie die *gefilterten* Datensätze aus der Log Manager-Datenbank. Dazu wählen Sie **Gefiltertes Protokoll löschen** aus dem Menü **Datei**. Diese Aktion kann *nicht* rückgängig gemacht werden.

  Wenn Sie einen Filter angewendet haben, wird die angezeigte Untergruppe der Datensätze permanent entfernt. Informationen zum Filtern der Log Manager-Datenbank finden Sie auf Seite 248.

- Entfernen Sie *alle* Datensätze aus der Log Manager-Datenbank. Dazu wählen Sie **Vollständiges Protokoll löschen** aus dem Menü **Datei**. Diese Aktion kann *nicht* rückgängig gemacht werden.

Weitere Installationsszenarien A

Installieren der Software auf einem Cluster Server

Sie können GroupShield für Exchange auf einem Microsoft Cluster Server installieren. Microsoft Cluster Server ist ein integriertes Feature von Microsoft Windows NT Server 4.0, Enterprise Edition. Einzelheiten zur Konfiguration von Microsoft Cluster Server finden Sie in Ihrer Microsoft Windows NT-Dokumentation.

WICHTIG: Bei der Installation werden Sie möglicherweise an zwei Stellen gebeten, den Server neu zu starten: einmal zur Installation des Microsoft Windows Installers, wenn dieser auf dem Installationsserver noch nicht vorhanden ist, und einmal, um sicherzustellen, daß der Scanner auf Anforderung korrekt funktioniert. Weitere Informationen über die Notwendigkeit dieser Neustarts finden Sie auf der Network Associates-Website. Oder wenden Sie sich an Ihren McAfee "Technischer Support"-Händler.

Bevor Sie GroupShield für Exchange auf einem Microsoft Cluster Server installieren, müssen Sie sicherstellen, daß das System die folgenden Anforderungen erfüllt:

- Microsoft Windows NT 4.0 Enterprise Edition, mit Service Pack 4 oder höher oder Microsoft Windows 2000 ist installiert und wird ordnungsgemäß ausgeführt.
- Microsoft Cluster Server 1.0 ist installiert und wird ordnungsgemäß ausgeführt.
- Microsoft Exchange 5.5 mit Service Pack 3 ist installiert und wird ordnungsgemäß ausgeführt.
- Das Verzeichnis, in dem Sie GroupShield für Exchange installieren möchten, ist ein freigegebenes Laufwerk auf dem aktiven Knoten des Clusterservers.

  Der aktive Knoten ist der Server, der in der Spalte Status den Eintrag Online und im Clusteradministrator in der Spalte Besitzer seinen Computernamen anzeigt. Das als Installationsort von GroupShield für Exchange angegebene freigegebene Laufwerk muß für alle Knoten in der Clusterkonfiguration sichtbar sein. GroupShield für Exchange kann nicht auf dem lokalen Laufwerk eines Knotens installiert werden.

WICHTIG: GroupShield für Exchange 4.5 kann zur Zeit auf einem Cluster Server nicht von v4.0.4 auf v4.5 aktualisiert werden. McAfee empfiehlt, daß Sie alle vorherigen Versionen von GroupShield für Exchange vom Cluster Server entfernen, bevor Sie mit der Installation der Version 4.5 beginnen.

Gehen Sie wie folgt vor, um GroupShield für Exchange auf einem Microsoft Cluster Server zu installieren:

1. Navigieren Sie zum Installationsprogramm von GroupShield für Exchange, **SETUP.EXE**, auf einem freigegebenen Laufwerk auf dem aktiven Knoten und doppelklicken Sie darauf.

   McAfee empfiehlt, daß Sie die Software zuerst auf dem aktiven Knoten installieren. Wenn Sie den inaktiven Knoten als primären Server wählen, fragt das Setup-Programm, ob Sie die Exchange-Gruppe auf diesen Knoten verschieben und mit der Installation fortfahren möchten oder zum anderen Knoten wechseln möchten. Wenn Sie zum anderen Knoten wechseln, müssen Sie SETUP.EXE erneut ausführen.

2. Führen Sie die Schritte Schritt 2 bis Schritt 5 auf Seite 35 aus, um die Installation mit Hilfe des Microsoft Windows Installers zu beginnen.

3. Geben Sie im Bildschirm Server-Setup den Namen der Cluster Server-Exchange-Gruppe und nicht den Namen des Servers selbst ein.

   Das gewählte Verzeichnis muß das freigegebene Laufwerk des Clusters sein. Wenn Sie ein Verzeichnis wählen, das sich nicht auf einem freigegebenen Laufwerk befindet, fordert Sie der Installer auf, ein Laufwerk im Cluster wählen.

   Klicken Sie auf **Weiter>**, um fortzufahren.

4. Führen Sie nun die Schritte Schritt 8 auf Seite 39 bis Schritt 19 auf Seite 44 in “Installieren von GroupShield für Exchange” aus, um die Installation auf dem aktiven Knoten fertigzustellen.

5. Klicken Sie auf **Fertigstellen**, um die Installation abzuschließen.

6. Wechseln Sie zum Clusteradministrator. Die folgenden Network Associates-Objekte werden in der Exchange-Gruppe angezeigt:

- Network Associates GroupShield für Exchange
- Network Associates GroupShield-Online-Aktualisierung.

7. Warten Sie, bis bei den beiden in Schritt 6 aufgelisteten Objekten in der Spalte Status der Eintrag **Online** angezeigt wird, bevor Sie zum inaktiven Knoten wechseln.

8. Um GroupShield für Exchange auf dem inaktiven Knoten zu installieren, müssen Sie ihn zum aktiven Knoten machen. Navigieren Sie dazu auf dem inaktiven Knoten zu **SETUP.EXE**, und doppelklicken Sie darauf.

   Das Setup-Programm erkennt, daß der Knoten inaktiv ist, und kann ihn automatisch aktivieren.

9. Klicken Sie im Begrüßungsbildschirm auf **Weiter>**, um die Installation zu starten.

   Die auf dem primären Server vorgenommenen Konfigurationseinstellungen werden beibehalten und auf dem jetzt aktiven Knoten in den Installationsbildschirmen angezeigt.

   ANMERKUNG: McAfee empfiehlt, daß Sie zum Verwalten des Dienstes GroupShield für Exchange dasselbe Administratorkonto wählen, das auch für den primären Server angegeben wurde.

10. Wenn die Installation beendet ist, klicken Sie auf **Fertigstellen**.

    WICHTIG: Damit die Software richtig installiert wird, werden Sie möglicherweise gebeten, den Server neu zu starten. McAfee empfiehlt, den Server neu zu starten, wenn Sie dazu aufgefordert werden.

Ergänzende Informationen

GroupShield für Exchange wird auf einem Microsoft Cluster Server an den folgenden Clusterorten installiert:

- Die Clusterressourcen von GroupShield für Exchange werden in derselben Clustergruppe wie Microsoft Exchange installiert.
- Die Programmdateien von GroupShield für Exchange werden auf dem freigegebenen Laufwerk installiert.
- Die folgenden gemeinsam genutzten McAfee-Komponenten werden als lokale Ressourcen auf jedem Knoten installiert, da jede Anwendung von mehreren McAfee-Virenschutzprodukten verwendet werden kann:
  - McAfee Outbreak Manager. Das Dienstprogramm Outbreak Manager wird als Network Associates-Dienst installiert.
  - McAfee Warnungs-Manager. Das Dienstprogramm Warnungs-Manager wird als Network Associates-Dienst installiert.

– Network Associates Log Service (Protokollierdienst). Die McAfee-Dienstprogramme Log Manager und Quarantine Manager werden als Protokollierdienst installiert. Protokolleinträge können jedoch zentral von jedem Knoten aus angezeigt werden.

Jede gemeinsam genutzte Komponentenanwendung muß separat auf jedem einzelnen Knoten konfiguriert werden. Alle auf einem Knoten festgelegten Regeln müssen den anderen Knoten im Cluster hinzugefügt werden.

- Wenn Sie die McAfee-Virusdefinitionsdateien (.DAT-Dateien) mit Hilfe des McAfee-Dienstprogramms AutoUpdate aktualisieren (siehe Kapitel 7, „Automatische Aktualisierung der .DAT-Dateien.“), müssen Sie angeben, daß Sie den Cluster Server aktualisieren möchten. Sie müssen nicht die einzelnen Clusterknoten angeben.

Entfernen der Software von einem Cluster Server

Um GroupShield für Exchange von einem Microsoft Cluster Server zu entfernen, verwenden Sie die Microsoft Windows Installer-Technologie. Um die Software aus einer Cluster Server-Konfiguration zu entfernen, muß die Exchange-Gruppe verschoben werden. McAfee empfiehlt, daß Sie die Exchange-Gruppe verschieben, wenn gerade wenig E-Mail-Verkehr stattfindet, da die Microsoft Exchange Server-Software nicht funktioniert, während die Exchange-Gruppe verschoben wird.

ANMERKUNG: Nach dem Entfernen von GroupShield für Exchange sind Ihre Benutzer allerdings ohne Schutz vor Virusangriffen, die von infizierten E-Mail-Anlagen weiterverbreitet werden. Entfernen Sie das Programm nur dann, wenn Sie sicher sind, daß Sie schnell ein Upgrade auf eine neue Version durchführen können.

Gehen Sie wie folgt vor, um GroupShield für Exchange aus einer Microsoft Cluster Server-Konfiguration zu entfernen:

1. Navigieren Sie auf dem aktiven Clusterknoten im GroupShield für Exchange-Programmverzeichnis zu **SETUP.EXE,** und doppelklicken Sie darauf.
2. Klicken Sie im Fenster Anwendung hinzufügen / entfernen auf die Option **Alles entfernen**. Klicken Sie auf **OK>**, um zu bestätigen, daß Sie die Anwendung entfernen möchten.
3. Wenn der Microsoft Windows Installer die Komponenten von GroupShield für Exchange aus Ihrem System entfernt hat, wechseln Sie zum inaktiven Knoten.

4. Navigieren Sie auf dem inaktiven Knoten im Programmverzeichnis von GroupShield für Exchange zu **SETUP.EXE**, und doppelklicken Sie darauf.

5. Der Installer meldet, daß der aktuelle Knoten inaktiv ist, und fragt, ob Sie die Exchange-Gruppe darauf verschieben möchten.

6. Klicken Sie auf **Ja**, um die Exchange-Gruppe zu verschieben, oder auf **Nein**, um den Entfernungsvorgang unter Verwendung von Windows Installer abzubrechen.

   Wenn Sie möchten, können Sie den inaktiven Knoten mit Hilfe des Clusteradministrators aktivieren.

7. Wiederholen Sie Schritt 2 und Schritt 3 weiter oben in diesem Abschnitt, und klicken Sie auf **Fertigstellen**, um die Dateien und Komponenten zu entfernen und Ihr System zu aktualisieren.

Installation von GroupShield für Exchange im Hintergrund

Sie können GroupShield für Exchange auf einem Microsoft Exchange-Server im Hintergrund installieren, so daß Sie während der Installation nicht anwesend sein müssen. Die Installation kann zu einem von Ihnen gewählten Zeitpunkt erfolgen, zu dem sie den Betriebsablauf am wenigsten stört.

Eine Installation im Hintergrund erfolgt in zwei Phasen: Zuerst müssen Sie eine Konfigurationsdatei für GroupShield für Exchange erstellen, indem Sie den ersten Teil des Setup-Assistenten für GroupShield für Exchange ausführen, um Konfigurationsdetails zu erhalten. Informationen hierzu finden Sie unter “Phase 1 - Ermitteln von Konfigurationsdetails für GroupShield für Exchange“ auf Seite 258. Anschließend müssen Sie die Windows Installer-Datei SETUP.MSI ausführen, um die Installation abzuschließen. Informationen hierzu finden Sie unter “Phase 2 - Ausführen der .GSE-Konfigurationsdatei“ auf Seite 259.

Sie können denselben Installationsvorgang im Hintergrund verwenden, um GroupShield für Exchange auf mehreren Servern zu installieren. Unter “Installieren von GroupShield für Exchange auf mehreren Servern“ auf Seite 260 finden Sie Informationen darüber, wie mehrere Installationen von GroupShield für Exchange v4.5 durchgeführt werden.

Systemanforderungen

Stellen Sie vor dem Installieren von GroupShield für Exchange sicher, daß die Installationszielserver die folgenden Eigenschaften aufweisen:

- Microsoft Exchange Administrator wird ordnungsgemäß ausgeführt.

ANMERKUNG: Auf dem Zielcomputer für GroupShield für Exchange muß nicht die vollständige Microsoft Exchange Server-Software installiert sein.

- Microsoft Windows Installer v1.1

  Die mit dem Installationspaket von GroupShield für Exchange gelieferte Datei INSTMSIW.EXE installiert Microsoft Windows Installer 1.1 automatisch.

ANMERKUNG: Der Windows Installer ist auf Windows 2000-Systemen standardmäßig installiert.

Die Datei INSTMSIW.EXE muß auf den Zielservern für GroupShield für Exchange aktiviert werden, damit der Windows Installer installiert wird. Speichern Sie dazu die Datei auf einem freigegebenen Netzlaufwerk, und wählen Sie dann auf dem Zielcomputer **Start>Ausführen**. Geben Sie `INSTMSI` in das Textfeld `Ausführen` ein.

Phase 1 - Ermitteln von Konfigurationsdetails für GroupShield für Exchange

Um die Konfigurationsdetails für GroupShield für Exchange zu ermitteln und eine Konfigurationsdatei zu erstellen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie auf Ihrem lokalen Server zur Datei **SETUP.EXE** von GroupShield für Exchange, und doppelklicken Sie darauf.
2. Führen Sie Schritt 8 auf Seite 39 bis Schritt 19 auf Seite 44 im Administratorhandbuch von GroupShield für Exchange v4.5 aus.

   Aus den in diesen Schritten ermittelten Informationen werden die Konfigurationsdetails von GroupShield für Exchange für die Konfigurationsdatei erstellt.
3. Klicken Sie im Bildschirm Installation beginnen auf **Abbrechen** und dann auf **Setup beenden**, um die Installation zu beenden.

   Im Verzeichnis Windows NT\Temp% wird eine Konfigurationsdatei namens <ORGANIZATION>$<SITE>$<SERVER>.GSE erstellt. Der Dateiname ist einmalig und kann nur verwendet werden, um GroupShield für Exchange auf dem Server zu installieren, den Sie im Bildschirm Server-Setup (Abbildung 2-3 auf Seite 37) ausgewählt haben.

ANMERKUNG: Wenn GroupShield für Exchange v4.0.4 beim Starten der Installation von GroupShield für Exchange v4.5 auf dem Server noch vorhanden ist, enthält die Konfigurationsdatei auch alle Konfigurationsdaten für Version 4.0.4.

Phase 2 - Ausführen der .GSE-Konfigurationsdatei

ANMERKUNG: McAfee empfiehlt, daß Sie eine Kopie der in "Phase 1 - Ermitteln von Konfigurationsdetails für GroupShield für Exchange" erstellten .GSE-Konfigurationsdatei erstellen, bevor Sie GroupShield für Exchange installieren.

Um den Installationsvorgang im Hintergrund mit Hilfe der vorher erstellten .GSE-Konfigurationsdatei auszuführen, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, daß auf dem Server, auf dem Sie GroupShield für Exchange installieren möchten, bereits eine SETUP.MSI-Datei vorhanden ist.

   Die Datei SETUP.MSI wird vom Windows Installer verwendet, um GroupShield für Exchange zu installieren. Wenn diese Datei auf dem Installationszielserver nicht vorhanden ist, führen Sie das im Abschnitt "Systemanforderungen" dieses Kapitels beschriebene Verfahren aus, um den Windows Installer zu installieren. Sie können GroupShield für Exchange nicht auf einem Computer installieren, auf dem die Datei SETUP.MSI nicht vorhanden ist.

   ANMERKUNG: Windows Installer 1.1 muß auf dem Server installiert sein, da sich sonst GroupShield für Exchange nicht installieren lässt.

2. Wählen Sie in der Windows NT-Taskleiste **Start > Ausführen**, und geben Sie in das Textfeld Ausführen den folgenden Befehl ein:

   ```
   MSIEXEC /Q /I <Pfad zur Datei SETUP.MSI>SETUP.MSI
   GSECONFIGDIR=<Verzeichnispfad zur Konfigurationsdatei>
   GSECURCONFIGFILE=<Name der Konfigurationsdatei>
   ```

   Falls erforderlich, können Sie den Befehl mit Hilfe eines Taskplaners zur Ausführung zu einem späteren Zeitpunkt planen.

ANMERKUNG: Die Variable <Pfad zur Datei SETUP.MSI> kann ein freigegebenes Netzlaufwerk oder der Verzeichnispfad auf dem lokalen Computer sein. Die Verzeichnisvariable GSECONFIGDIR sollte auf den Namen des Verzeichnisses (in Universal Notation Convention, UNC) eingestellt sein, in dem die .GSE-Datei enthalten ist, d. h. C:\TEMP oder \\SERVER1\GSE\CONFIGFILES. Geben Sie die spitzen Klammern < > nicht mit ein.

Die Verzeichnisvariable GSECURCONFIGFILE muß auf den Namen der .GSE-Konfigurationsdatei eingestellt werden, d. h. <ORGANIZATION> $<SITE>$<SERVER>.GSE.

Bei einer Hintergrund- oder Mehrfachinstallation wird der Server bei Bedarf automatisch neu gestartet. Sie werden nicht benachrichtigt, wenn die Installation abgeschlossen ist.

Installieren von GroupShield für Exchange auf mehreren Servern

Um GroupShield für Exchange auf mehreren Servern zu installieren, müssen Sie für jeden Zielserver eine <ORGANIZATION>$<SITE>$<SERVER>.GSE-Datei erstellen. Informationen über das Erstellen einer .GSE-Datei finden Sie unter “Phase 1 - Ermitteln von Konfigurationsdetails für GroupShield für Exchange“ auf Seite 258.

Zum Erstellen mehrerer <ORGANIZATION>$<SITE>$<SERVER>.GSE-Konfigurationsdateien führen Sie die folgende Schritte aus:

1. Führen Sie die Schritte in “Phase 1 - Ermitteln von Konfigurationsdetails für GroupShield für Exchange“ auf Seite 258 aus, bis der Bildschirm Installation beginnen angezeigt wird. Klicken Sie jedoch NICHT auf **Abbrechen**.
2. Klicken Sie stattdessen im Bildschirm Installation beginnen auf **<<Zurück**, bis wieder der Bildschirm Server-Setup angezeigt wird (Abbildung 2-3 auf Seite 37).
3. Wählen Sie hier einen anderen Server aus, auf dem Sie GroupShield für Exchange installieren möchten.
4. Geben Sie im Setup-Assistenten die Konfigurationsinformationen zu dem in Schritt 2 gewählten Server ein, bis wieder der Bildschirm **I**nstallation beginnen angezeigt wird.

Jetzt können Sie entweder diesen Vorgang wiederholen, bis für jeden Installationszielserver eine <ORGANIZATION>$<SITE>$<SERVER>.GSE-Datei vorhanden ist, oder mit Schritt 5 fortfahren.

5. Wechseln Sie zum Remote-Server, und führen Sie die Schritte in “Phase 2 - Ausführen der .GSE-Konfigurationsdatei“ auf Seite 259 aus, um GroupShield für Exchange zu installieren.

   Sie werden nicht benachrichtigt, wenn die Installation abgeschlossen ist. Um zu prüfen, ob GroupShield für Exchange richtig installiert ist und Viren erkennt, führen Sie die Schritte in “Testen einer Installation“ auf Seite 44 aus. Um zu prüfen, ob der Microsoft Exchange-Server die richtigen Attribute für GroupShield für Exchange aufweist, lesen Sie bitte die Informationen unter “Änderungen am System nach Abschluß der Installation“ auf Seite 46.

McAfee-Aktualisierungsdienstprogramme

B

Aktuelle McAfee Aktualisierungsdienstprogramme

Die Aufgabe, eine Aktualisierungsstrategie für .DAT-Dateien zu entwickeln, die alle Gegebenheiten Ihrer Betriebssystemumgebung und Ihre Sicherheitsanforderungen berücksichtigt, kann abschreckend wirken. Zusätzlich zu den Informationen in Kapitel 7, “Automatische Aktualisierung der .DAT-Dateien,” werden im vorliegenden Anhang Erweiterungen zu AutoUpdate und die verschiedenen McAfee-Zeitplandateien und -dienstprogramme behandelt, die Sie zusammen mit AutoUpdate einsetzen können, um Ihr McAfee-Virenschutzprogramm schnell und effizient zu aktualisieren.

Es gibt vier unterschiedliche Wege zum Aktualisieren der .DAT-Dateien und der Moduldateien in Ihrem Netzwerk. Es folgt eine grobe Übersicht über diese Methoden mit Informationen dazu, nach welchen Gesichtspunkten Sie die für ihre Aktualisierungsanforderungen am besten geeignete Methode auswählen.

Aktualisieren von .DAT-Dateien und Moduldateien

Sie können die .DAT-Datei und die Engine-Datei gleichzeitig mit dem Dienstprogramm McAfee SuperDAT aktualisieren.

Das Dienstprogramm SuperDAT installiert Aktualisierungen am Scanmodul und an den .DAT-Dateien, die Ihre Virenschutzsoftware zum Identifizieren und Entfernen infizierter Dateien verwendet. Das Dienstprogramm SuperDAT beendet alle aktiven Scanvorgänge, Dienste oder andere speicherresidente Softwarekomponenten, die mit Ihren Aktualisierungen in Konflikt geraten könnten. Anschließend kopiert es die neuen Dateien an die entsprechenden Stellen und veranlaßt, daß sie Ihre Software sofort verwendet.

Diese Aktualisierung erfolgt für den Endbenutzer transparent. Nach Abschluß der Aktualisierung erhält der Benutzer die Aufforderung, das System neu zu starten. Weitere Informationen hierzu finden Sie in der in jedem SuperDAT-Download enthaltenen README.TXT-Datei.

Einschränkungen:

- Zwar empfiehlt McAfee den Einsatz dieses Dienstprogramms als wirkungsvolles Hilfsmittel zum Aktualisieren sowohl des Virenschutzmoduls als auch der .DAT-Dateien, es muß jedoch berücksichtigt werden, daß mit dem Dienstprogramm SuperDAT keine *inkrementellen* Aktualisierungen der .DAT-Dateien möglich sind.

- Da die aktuelle Version des Hilfsprogramm SuperDAT inkrementelles Aktualisieren der .DAT-Dateien nicht unterstützt, empfiehlt McAfee, die Virenschutzdateien Ihrer Virenschutz-Software mit Hilfe von AutoUpdate zu aktualisieren. Siehe Kapitel 7, “Automatische Aktualisierung der .DAT-Dateien”.

Aktualisieren nur der Moduldateien Ihrer Virenschutzsoftware

In bestimmten Fällen muß der Administrator zuerst die Moduldateien aktualisieren und die Aktualisierungen der .DAT-Dateien vorbereiten und später manuell durchführen. Es kann Fälle geben, in denen die Moduldatei-Aktualisierungen nicht an Endbenutzer weitergegeben werden sollen.

Verwenden von SuperDAT

Wenn Sie Zugriff auf SuperDAT 1.2 oder höher haben, können Sie die Engine-Aktualisierungsdateien auf einen Primärserver downloaden und dann die Aktualisierungsdateien unter Verwendung von SuperDAT oder Microsoft Systems Management Server (SMS) bereitstellen, damit diese intern implementiert werden können.

Das Dienstprogramm SuperDAT installiert Aktualisierungen am Scanmodul und an den .DAT-Dateien, die Ihre Virenschutzsoftware zum Identifizieren und Entfernen infizierter Dateien verwendet. Das Dienstprogramm SuperDAT beendet alle aktiven Scanvorgänge, Dienste oder andere speicherresidente Softwarekomponenten, die mit Ihren Aktualisierungen in Konflikt geraten könnten. Anschließend kopiert es die neuen Dateien an die entsprechenden Stellen und veranlaßt, daß sie Ihre Software sofort verwendet.

Diese Aktualisierung erfolgt für den Endbenutzer durchgehend transparent. Nach Abschluß der Aktualisierung erhält der Benutzer die Aufforderung, das System neu zu starten. Weitere Informationen zur Verwendung des Dienstprogramms SuperDAT finden Sie in der in jedem SuperDAT-Download enthaltenen README.TXT-Datei.

❑ **ANMERKUNG:** Windows NT-Benutzer können mit Hilfe von SuperDAT 1.2 die .DAT-Dateien aktualisieren, ohne die Dienste herunterfahren zu müssen, da das Dienstprogramm SuperDAT nicht über Benutzerrechte, sondern über Systemrechte verfügt.

Verwenden von SecureCast

SecureCast ist ein Dienst für Netzwerkadministratoren, der Virenschutz-Upgrades und -Aktualisierungen sowie Viruswarnungen automatisch an den Desktop des Administrators liefert. Umfassende Informationen zu diesem Dienst finden Sie auf der SecureCast-Website unter

http://www.nai.com/asp_set/anti_virus/updates/secure.asp

Aktualisieren nur der .DAT-Dateien aus den .DAT-Archiven

Die regulären .DAT-Dateien (SCAN.DAT, NAMES.DAT und CLEAN.DAT) werden wöchentlich bereitgestellt und können von der Network Associates FTP-Site oder Website unter Verwendung des Dienstprogramms AutoUpdate gedownloadet werden. Diese Dateien aktualisieren nur die von Ihrer Software zur Virenerkennung und zum Löschen von Viren verwendeten Virenschutzdateien, sie upgraden nicht die Virenschutzsoftware selbst.

Es gibt zwei Möglichkeiten, aus den .DAT-Dateiarchiven heraus zu aktualisieren. Obwohl McAfee empfiehlt, zum Downloaden und automatischen Aktualisieren dieser .DAT-Dateien das Dienstprogramm AutoUpdate zu verwenden, kann der Benutzer die Dateien auch manuell downloaden und den Aktualisierungsprozeß zu einem beliebigen späteren Zeitpunkt selber durchführen. Damit erhält der Administrator mehr Kontrolle über den Prozeß der Aktualisierung der .DAT-Dateien im Hinblick auf das Downloaden und Verteilen der Dateien, als bei der Bereitstellungsmethode (push) der anderen McAfee-Dienstprogramme.

Spezielle Aktualisierungsmechanismen

. **WICHTIG:** Die folgenden Dienstprogramme wurden von AVERT für den Einsatz zwischen den wöchentlichen .DAT-Veröffentlichungen entwickelt. Diese Dienstprogramme bieten Hilfestellung bei verschiedenen Problemen und sollten wie von Ihrem McAfee-Händler empfohlen verwendet werden. Bei diesen AVERT-Dateien handelt es sich nicht um veröffentlichte Produkte: Sie wurden nicht von der Qualitätssicherung genehmigt und können falsche Alarme auslösen oder sogar Systemabstürze auf Ihren Computern verursachen.

- EXTRA.DAT—Dies ist eine kleinere zusätzliche Virenschutzdatei, die bei Bedarf zwischen den regulären wöchentlichen .DAT-Aktualisierungen bereitgestellt wird als Maßnahme gegen eine Virenepidemie, wie z.B. der E-Mail-Virus W97M/MELISSA. Sie kann manuell oder mit Hilfe des Dienstprogramms SuperDAT installiert werden. Weitere Informationen und Installationsanweisungen finden Sie in der jedem EXTRA.DAT-Release beigefügten README.TXT-Datei.
- Vorabversionen der v4.x.xx-.DAT-Dateien—Die neuesten v4.x.xx-.DAT-Dateien aus den AVERT-Forschungslabors unter:

  http://www.nai.com/asp_set/anti_virus/avert/tools.asp

- Erste-Hilfe-.DAT-Dateiaktualisierungen—Dies sind v4.x.xx-.DAT-Dateien in reduzierter Größe, die auf eine 1,44-MB-Diskette passen. Downloaden Sie diese Dateien direkt auf Ihre Erste-Hilfe-Diskette, um infizierte Systeme neu zu starten und zu säubern. Sie erhalten Sie unter:

  http://www.nai.com/asp_set/anti_virus/avert/tools.asp

Die neueste Aktualisierungserweiterung: inkrementelle .DAT-Dateien

Während Kapitel 7, “Automatische Aktualisierung der .DAT-Dateien” Informationen zur Verwendung der AutoUpdate-Komponente enthält, erläutert der vorliegende Abschnitt die jetzt neue Funktion zum Durchführen inkrementeller .DAT-Dateiaktualisierungen. Für viele Administratoren werden die Aufgaben im Rahmen der .DAT-Aktualisierung mit dieser Funktionserweiterung deutlich einfacher.

Es ist wichtig, daß zuerst die vom Modul zum Scannen verwendeten Dateien aktualisiert werden. Anschließend können dann die Virusdatendateien (.DAT) selbst aktualisiert werden. Wenn aktuelle .DAT-Dateien in veralteter Software verwendet werden, kann das Modul die Dateien u. U. nicht optimal nutzen. Bis zur Behebung dieser Situation kann es zu Lücken im Schutz ihrer Daten kommen.

Für Benutzer von GroupShield für Exchange stehen mehrere Aktualisierungsdienstprogramme zur Verfügung. Einen Überblick finden Sie unter “Aktuelle McAfee Aktualisierungsdienstprogramme” auf Seite 263. Da jede Netzwerkkonfiguration ihre eigenen speziellen Herausforderungen birgt, empfiehlt McAfee Administratoren, beim Upgraden einer veralteten McAfee Virenschutz-Software die folgenden Punkte zur berücksichtigen:

- Wenn Ihre Virenschutzsoftware auf mehreren Servern ausgeführt wird, empfiehlt McAfee einen zweistufigen Prozeß: Downloaden der Aktualisierung und der DELTA.INI-Dateien auf einen einzelnen Server und anschließend Initiieren eines internen Downloads und Verteilen der Daten. Anschließend sind die Moduldateien Ihrer Virenschutzsoftware auf dem neuesten Stand.
- Jetzt können Sie mit Hilfe der neuen Funktion der AutoUpdate-Komponente die von Ihrer Software verwendeten .DAT-Dateien inkrementell aktualisieren. Von diesem Zeitpunkt an verwenden Sie AutoUpdate, um automatisch *inkrementelle* Downloads der erforderlichen Virenschutzdateien zu starten. Dies führt zu einer deutlichen Reduzierung der Downloadzeiten und des entsprechenden Verwaltungsaufwands.

Was ist eine inkrementelle .DAT-Aktualisierung?

Alle Virenschutzprodukte müssen regelmäßig aktualisiert werden. Nur dann ist gewährleistet, daß die Virusdefinitionsdateien (.DAT) die neusten Informationen enthalten. In früheren Versionen des Dienstprogramms AutoUpdate mußte jedesmal, wenn ein Benutzer eine Aktualisierung der .DAT-Dateien initiierte, das gesamte Virussignaturpaket gedownloadet werden.

Um die Größe des Downloads und die Verbindungszeiten zu reduzieren, wurde die AutoUpdate-Funktion Ihrer Virenschutzsoftware verbessert. Das Dienstprogramm AutoUpdate unterstützt jetzt die inkrementelle Aktualisierung dieser extrem wichtigen .DAT-Dateien: Es wird nur das gedownloadet, was sich seit dem letzten Aktualisieren der .DAT-Dateien geändert hat. Damit wird der Prozeß der .DAT-Aktualisierung wesentlich effizienter. Die Downloads, die die Virenschutz-Software benötigt, um gegen neueste Viren wirken zu können, sind damit deutlich kleiner.

Diese leistungsstarke Erweiterung erfordert vom Benutzer nur wenig Aufwand. Nach dem Konfigurieren und Initiieren führt AutoUpdate automatisch eine inkrementelle Aktualisierung durch.

Das Dienstprogramm AutoUpdate prüft, welche Aktualisierungsdateien Ihr System benötigt und beginnt, diese zu downloaden. Wenn der inkrementelle Download oder der Aktualisierungsprozeß fehlschlägt, wird standardmäßig ein vollständiger .DAT-Download mit anschließender Aktualisierung durchgeführt.

Funktionen der inkrementellen Aktualisierung

- Die neue Funktionalität basiert auf vorhandenen AutoUpdate-Protokollen. Auf den Clientcomputern sind keine Konfigurationsänderungen erforderlich.
- Der AutoUpdate-Zeitplan enthält jetzt eine Funktion zum willkürlichen Festlegen der Aktualisierungszeit. Siehe hierzu “Zeitliche Planung der Aktualisierungen” auf Seite 136.
- Die durchschnittliche Downloadgröße wurde von 3 MB auf 100-110 KB reduziert. (Die Größe der inkrementellen *.UPD-Dateien kann naturgemäß schwanken.)

Einschränkungen der inkrementellen Aktualisierung

- Eine inkrementelle Aktualisierung verläuft nur dann erfolgreich, wenn Ihre Virenschutz-Software über eine aktualisierte Modul, 4.0.50 oder höher, verfügt. Welche Engine enthalten ist, sehen Sie auf der Registerkarte Version von GroupShield für Exchange. Siehe Seite 122.
- Statt einer inkrementellen .DAT-Aktualisierung wird nur dann standardmäßig eine vollständige .DAT-Aktualisierung durchgeführt, wenn sich sowohl die Dateien für die inkrementelle Aktualisierung als auch die regulären .DAT-Zip-Dateien im Aktualisierungsverzeichnis befinden, das der Benutzer in den Eigenschaften für das Dienstprogramm AutoUpdate angegeben hat.

- In dieser Version von GroupShield für Exchange enthält die AutoUpdate-Erweiterung die Funktionalität für inkrementelle Aktualisierung der .DAT-Dateien, nicht jedoch für inkrementelle Aktualisierung der Engine-Dateien.
- Wenn Sie das McAfee-Dienstprogramm SuperDAT zum Aktualisieren sowohl des Moduls als auch der .DAT-Dateien verwenden, wird ein *vollständiger*, nicht ein inkrementeller Download der Daten initiiert, die benötigt werden, damit sowohl die Virenschutzsoftware als auch die .DAT-Dateien auf dem neuesten Stand sind. Sobald Ihre Virenschutzsoftware auf dem neuesten Stand ist, kann die AutoUpdate-Funktion inkrementelle Downloads initiieren.

Wie funktioniert die inkrementelle Aktualisierung von .DAT-Dateien?

Die AutoUpdate-Funktion verwendet die beiden während des Aktualisierungsprozesses gedownloadeten Dateitypen, um die lokalen .DAT-Dateien sorgfältig zu aktualisieren. Jeder inkrementelle .DAT-Download besteht aus den folgenden Dateien:

- *.UPD-Dateien—Diese Aktualisierungsdateien enthalten nur die Änderungen zwischen einer Gruppe von .DAT-Dateien und der nachfolgenden. Der Dateiname jeder *.UPD-Datei besteht aus der Nummer der Basis-.DAT-Datei (z.B. 4064) und der nächsten .DAT-Version sowie der Erweiterung .UPD. Eine Datei zum Aktualisieren der DAT-Gruppe 4064 auf 4065 hat damit den Namen 40644065.UPD.
- Eine DELTA.INI-Datei—Dies ist eine Steuerungsdatei mit Informationen zu den verfügbaren .UPD-Dateien, Dateigrößen und Validierungscodes. Die Datei DELTA.INI wird mit jeder wöchentlichen .DAT-Bereitstellung aktualisiert. Für jede .DAT-Version wird ein Eintrag zur DELTA.INI-Datei hinzugefügt.

  Die Datei hat folgendes Format:

```
[DELTAS]
4050=I001.UPD
4051=I002.UPD
4052=I003.UPD
4053=I004.UPD
```

Anhand dieser Informationen ermittelt das Dienstprogramm AutoUpdate, welche .UPD-Dateien zum Aktualisieren der derzeit installierten .DAT-Dateien erforderlich sind, und um sicherzustellen, daß die gedownloadeten Dateien nicht geändert wurden oder beschädigt sind. Wenn AutoUpdate z. B. auf Ihrem lokalen System die vollständige .DAT-Gruppe mit der Nummer 4052 findet, gibt die Datei DELTA.INI an, daß die inkrementelle .DAT-Date I003 gedownloadet wird.

Das Dienstprogramm AutoUpdate prüft, welche *.UPD-Dateien Ihr System benötigt, und beginnt, diese zu downloaden. Anschließend werden die vorhandenen .DAT-Dateien decodiert, die inkrementellen .DAT-Aktualisierungen ordnungsgemäß implementiert, die Daten überprüft und die aktualisierten .DAT-Dateien wieder codiert.

Tips

Interne im Vergleich zu externen Quellen

Aktualisierte .DAT-Dateien befinden sich standardmäßig in Verzeichnissen der Network Associates FTP-Site oder -Website. Einige Firmen erlauben jedoch nicht allen Mitarbeitern vollständigen Webzugriff oder beschränken Downloadzeiten auf ein Minimum. McAfee empfiehlt das Downloaden von .DAT-Dateien auf einen Server und das Verteilen der Dateien in internen Netzwerken. Damit können die gedownloadeten .DAT-Dateien lokal abgerufen werden.

Sie können für diese Aufgabe einen internen FTP-Server einrichten oder die inkrementellen Aktualisierungen direkt von einem UNC-Share auf einen Microsoft Windows NT-Server downloaden. Konfigurationsdetails finden Sie unter Schritt auf Seite 133. Anschließend können mit dem Dienstprogramm AutoUpdate interne Aktualisierungen von diesem primären Server aus geplant werden.

❑ **ANMERKUNG:** Wenn *.UPD-Dateien auf einen internen Standort gedownloadet werden, müssen Sie sicherstellen, daß auch die neuste Version der Datei DELTA.INI gedownloadet wird. Markieren Sie keine der Dateien als schreibgeschützt, da der Zielcomputer dann später bei dem Versuch, die Datei zu löschen, u. U. eine Fehlermeldung ausgibt.

Planen interner .DAT-Aktualisierungen

Sie können den primären Server des Kunden entweder automatisiert oder manuell aktualisieren. Umfassende Informationen zu den Planungsoptionen des Dienstprogramms AutoUpdate finden Sie unter “Zeitliche Planung der Aktualisierungen” auf Seite 136.

WICHTIG: Für Clientaktualisierungen empfiehlt es sich, einen Termin zu planen, der nach der Bestätigung liegt, daß der .DAT-Datei-Download von der Network Associates FTP-Site oder -Website abgeschlossen ist. Andernfalls kann es sein, daß Ihre Virenschutzsoftware anschließend nicht mehr auf dem neuesten Stand ist.

Neue .DAT-Planungsfunktion

Der Aktualisierungsprozeß enthält eine neue Planungsfunktion, die eine Aktualisierung innerhalb von einer Stunde vor und nach der angegeben Zeit willkürlich festlegt. Damit wird verhindert, daß alle Clientcomputer gleichzeitig versuchen, eine Aktualisierung durchzuführen. Beispiel:

- Konfigurieren Sie eine geplante Aktualisierung für 22.00 Uhr.
- Aktivieren Sie die Funktion für willkürliche Planung. (Details zu dieser und anderen AutoUpdate-Planungsfunktionen finden Sie unter “Zeitliche Planung der Aktualisierungen” auf Seite 136.)
- Auf dem Clientcomputer erfolgt die geplante Aktualisierung dann zwischen 21:00 und 23:00.

❑ **ANMERKUNG:** Stellen Sie sicher, daß Sie eine Clientaktualisierung so planen, daß sie erst nach Bestätigung des vollständigen Downloads von der Network Associates FTP-Site oder -Website erfolgt.

Häufig gestellt Fragen

Verbindungsprobleme

F: Was geschieht, wenn mein Computer während einer geplanten Aktualisierung ausgeschaltet ist?

A: Wenn ein geplantes Ereignis fehlt, weil der Computer zur entsprechenden Zeit ausgeschaltet wurde, wird das Ereignis beim nächsten Systemstart automatisch gestartet.

F: Was geschieht, wenn die Internet-/Netzwerkverbindung während einer Aktualisierung unterbrochen wird?

A: Die inkrementellen Dateien, die vor Unterbrechung der Verbindung gedownloadet wurden, werden implementiert, und der Fehler beim Downloaden der verbleibenden Inkremente wird im Aktivitätsprotokoll aufgezeichnet.

Beschädigte Daten

F: Was geschieht, wenn eine der inkrementellen Dateien während des Downloads beschädigt wird?

A: Jede inkrementelle Datei wird vor dem Implementieren der Änderungen anhand einer Prüfsumme aus der Datei DELTA.INI überprüft. Wenn die Prüfsumme nicht identisch ist, werden die in dieser Datei enthaltenen Änderungen und alle nachfolgenden in dieser Sitzung gedownloadeten inkrementellen Dateien nicht implementiert. Stattdessen wird ein Fehlerdialogfeld angezeigt und AutoUpdate führt für diese Aktualisierungssitzung mit einen vollständigen Download einer .DAT-Datengruppe durch.

Inkrementelle im Gegensatz zu vollständiger Aktualisierung

F: Was geschieht, wenn meine .DAT-Dateien extrem veraltet sind? Funktioniert auch dann eine inkrementelle Aktualisierung?

A: Das Dienstprogramm AutoUpdate entscheidet, welcher Prozeß verwendet werden muß. Hier ist kein Eingriff von Benutzerseite erforderlich. Der inkrementelle Prozeß wird nur zum Aktualisieren von .DAT-Dateien verwendet, die nicht älter als 15 Wochen sind. Ab diesem Zeitpunkt ist es effizienter, eine vollständige Gruppe von .Dat-Dateien zu downloaden.

Netzwerkkonfigurationsprobleme

F: Müssen alle Computer, die aktualisiert werden sollen, eine Verbindung zum Internet haben?

A: Nein. Konfigurieren Sie einen Computer im Netzwerk zum Downloaden der Dateien aus dem Internet. Die anderen Computer in Ihrem Netzwerk können die Aktualisierungen dann von diesem Computer abrufen. Genaue Informationen zu diesem Prozeß finden Sie unter “Aktualisieren der Virusdefinitionsdateien (.DAT-Dateien) von einem entfernten Server aus” auf Seite 134.

F: Wie kann ich Netzwerkengpässe vermeiden, wenn mehrere Workstations aktualisiert werden müssen?

A: Der AutoUpdate-Zeitplan unterstützt eine Funktion zur willkürlichen Planung von Aktualisierungszeiten, mit der Sie die Netzwerklast verteilen können. Genaue Informationen zu dieser Funktion finden Sie unter “Zeitliche Planung der Aktualisierungen” auf Seite 136.

Planungsprobleme

F: Wie oft muß ich prüfen, ob Aktualisierungen vorliegen?

A: McAfee stellt in der Regel wöchentlich aktualisierte .DAT-Dateien zur Verfügung. Sie können jedoch je nach ihren speziellen Sicherheitsanforderungen öfter oder seltener prüfen, ob Aktualisierungen vorliegen. Beachten Sie jedoch, daß Ihr Risiko einer Vireninfektion steigt, wenn die Abstände zwischen den Aktualisierungen der Virusdatendateien zu groß sind.

Benutzerschulung

F: Muß ich die Benutzer für die Durchführung von inkrementellen Aktualisierungen schulen?

A: Nein. Die inkrementelle Aktualisierung wurde nahtlos in die vorhandene AutoUpdate-Funktion integriert.

Dateinamen

F: Die Namen der verschiedenen Aktualisierungsdateien sind für mich neu. Wie lautet die entsprechende Benennungskonvention?

A: Informationen zu den Namen der Aktualisierungsdateien finden Sie unter “Wie funktioniert die inkrementelle Aktualisierung von .DAT-Dateien?” auf Seite 268.

McAfee-Supportdienste C

Die Wahl von McAfee Virenschutz- und Sicherheitssoftware hilft Ihnen sicherzustellen, daß die entscheidende Informationstechnologie, auf die Sie sich verlassen, reibungslos und effizient funktioniert. Das Nutzen eines McAfee-Supportplans erweitert den Schutz, den Ihre Software Ihnen bietet, indem er Ihnen Zugang zu dem Fachwissen gibt, das Sie brauchen, um Ihr System mit der neuesten Technologie von McAfee zu installieren, zu überwachen, zu pflegen und zu aktualisieren. Mit einem speziell auf Ihre Anforderungen zugeschnittenen Support-Plan können Sie sicherstellen, daß Ihr System oder Ihr Netzwerk über Monate und Jahre sicher läuft.

Supportpläne von McAfee fallen in zwei Hauptkategorien. Als Geschäftskunde können Sie im McAfee Corporate PrimeSupport-Programm unter vier Stufen eines erweiterten Supports wählen. Wenn Sie ein Produkt von McAfee im Einzelhandel erworben haben, können Sie aus dem Retail PrimeSupport-Programm einen Plan wählen, der auf Ihre Bedürfnisse abgestimmt ist.

PrimeSupport-Optionen für Firmenkunden

Beim PrimeSupport-Programm von McAfee haben Sie die Wahl zwischen den folgenden Optionen: KnowledgeCenter, Connect und Enterprise. Jede Option verfügt über Leistungsmerkmale, die Ihnen einen kosteneffektiven und raschen Support bieten, der auf Ihre Bedürfnisse zugeschnitten ist.

PrimeSupport KnowledgeCenter

Das PrimeSupport KnowledgeCenter bietet Ihnen Zugang zu technischer Unterstützung über eine McAfee-Online-Wissensdatenbank sowie Produktaktualisierungen über die McAfee-Website. Wenn Sie Ihr Produkt von McAfee mit einer Abonnementlizenz erworben haben, erhalten Sie je nach Länge des Abonnements PrimeSupport KnowledgeCenter als Teil des Pakets für einen Zeitraum von zwei Jahren ab Kaufdatum. Wenn Sie Ihr Produkt von McAfee mit einer Jahreslizenz erworben haben, können Sie Ihren PrimeSupport KnowledgeCenter-Plan gegen eine jährliche Gebühr erneuern.

Um das KnowledgeCenter-Kennwort zu erhalten oder Ihren PrimeSupport-Vertrag bei McAfee zu registrieren, besuchen Sie:

http://knowledge.nai.com/

Das ausgefüllte Formular wird an das Network Associates-Kundendienstcenter weitergeleitet. Sie müssen dieses Formular ausfüllen, ehe Sie sich mit dem PrimeSupport KnowledgeCenter verbinden oder den Network Associates PrimeSupport anrufen können.

Einzelheiten zu PrimeSupport KnowledgeCenter:

- Online-Zugriff auf technische Lösungen in einer durchsuchbaren Wissensdatenbank, elektronische Vorfallübermittlung und technische Dokumente wie Benutzerhandbücher, Kataloge mit häufig gestellten Fragen und Versionsinformationen
- Unbeschränkter Rund-um-die-Uhr-Zugriff auf die Informationen des technischen Supports über die Website von McAfee
- Updates für Datendateien und Produkt-Upgrades über die Website von McAfee

PrimeSupport Connect

PrimeSupport Connect bietet Ihnen telefonischen Zugriff auf grundlegende Produktunterstützung durch erfahrene Mitarbeiter im technischen Support von McAfee.

Einzelheiten zu PrimeSupport Connect:

- Unbegrenzter gebührenfreier telefonischer Zugriff auf technischen Support von Montag bis Freitag von 08.00 bis 20.00 Uhr amerikanischer Zentralzeit
- Online-Zugriff auf technische Lösungen in einer durchsuchbaren Wissensdatenbank, elektronische Vorfallübermittlung und technische Dokumente wie Benutzerhandbücher, Kataloge mit häufig gestellten Fragen und Versionsinformationen
- Unbeschränkter Rund-um-die-Uhr-Zugriff auf die Informationen des technischen Supports über die Website von McAfee
- Updates für Datendateien und Produkt-Upgrades über die Website von McAfee

PrimeSupport Priority

PrimeSupport Priority bietet Ihnen rund um die Uhr telefonischen Zugriff auf grundlegende Produktunterstützung durch erfahrene Mitarbeiter im technischen Support von McAfee. Sie können PrimeSupport Priority auf jährlicher Basis erwerben, wenn Sie ein Produkt von McAfee mit einer Abonnement- oder Jahreslizenz erwerben.

Einzelheiten zu PrimeSupport Priority:

- Unbegrenzter gebührenfreier telefonischer Zugriff auf technischen Support von Montag bis Freitag von 08.00 bis 20.00 Uhr amerikanischer Zentralzeit
- Bevorzugte Anrufbearbeitung während der Geschäftszeiten
- Betreuung außerhalb der Geschäftszeiten bei dringenden Problemen innerhalb einer Stunde auch an Wochenenden und Feiertagen
- Online-Zugriff auf technische Lösungen in einer durchsuchbaren Wissensdatenbank, elektronische Vorfallübermittlung und technische Dokumente wie Benutzerhandbücher, Kataloge mit häufig gestellten Fragen und Versionsinformationen
- Unbeschränkter Rund-um-die-Uhr-Zugriff auf die Informationen des technischen Supports über die Website von McAfee
- Updates für Datendateien und Produkt-Upgrades über die Website von McAfee

PrimeSupport Enterprise

PrimeSupport Enterprise bietet Ihnen rund um die Uhr persönlichen, aktiven Support von einem zugeteilten Mitarbeiter des technischen Supports. Sie werden den guten Kontakt mit einem Supportprofi schätzen, der sich mit dem Einsatz Ihres McAfee-Produkts im Netzwerk und mit bislang an ihn gestellten Supportfragen auskennt und Sie in Zeitabständen, die Sie selbst bestimmen, anruft, um sicherzugehen, daß Sie die nötigen Kenntnisse haben, um Produkte von McAfee zu nutzen und zu verwalten. Indem er Sie im voraus anruft, kann der Betreuer von PrimeSupport Enterprise Ihnen helfen, Probleme zu vermeiden, bevor sie entstehen. Für den Notfall bietet PrimeSupport Enterprise Ihnen eine garantierte Antwortfrist, so daß Sie sicher sein können, daß Hilfe unterwegs ist. Sie können PrimeSupport Enterprise auf jährlicher Basis erwerben, wenn Sie ein Produkt von McAfee mit einer Abonnement- oder Jahreslizenz erwerben.

Einzelheiten zu PrimeSupport Enterprise:

- Unbegrenzter gebührenfreier telefonischer Zugriff auf einen Mitarbeiter des technischen Supports rund um die Uhr an sieben Tagen in der Woche, einschließlich Wochenenden und Feiertagen
- Aktiver Supportkontakt durch Ihren Supportbetreuer über Telefon oder E-Mail in Zeitabständen, die Sie selbst bestimmen

- Zugesicherte Antwortzeiten: Ihr Supportbetreuer antwortet innerhalb einer halben Stunde auf Fragen über Pager, innerhalb einer Stunde auf Fragen, die per Voice Mail hinterlassen werden, und innerhalb von vier Stunden auf E-Mail-Anfragen
- Möglichkeit, mindestens fünf Mitarbeiter Ihres Unternehmens als Kundenkontaktpersonen zu benennen
- Die Option, als Beta-Standort für neue McAfee-Produkte zu fungieren
- Online-Zugriff auf technische Lösungen in einer durchsuchbaren Wissensdatenbank, elektronische Vorfallübermittlung und technische Dokumente wie Benutzerhandbücher, Kataloge mit häufig gestellten Fragen und Versionsinformationen
- Unbeschränkter Rund-um-die-Uhr-Zugriff auf die Informationen des technischen Supports über die Website von McAfee
- Updates für Datendateien und Produkt-Upgrades über die Website von McAfee

Bestellen von Corporate PrimeSupport

So bestellen Sie PrimeSupport KnowledgeCenter, PrimeSupport Connect, PrimeSupport Priority oder PrimeSupport Enterprise für Ihre McAfee-Produkte:

- Wenden Sie sich an den Händler, oder
- Rufen Sie in Nordamerika die Supportdienste von Network Associates Montag bis Freitag zwischen 6.00 Uhr und 17.00 Uhr pazifischer Zeit unter (800) 988-5737 oder (650) 473-2000 an.

> **ANMERKUNG:** Das in diesem Handbuch beschriebene PrimeSupport-Programm ist nur in Nordamerika erhältlich. Informationen über die PrimeSupport-Optionen, die außerhalb Nordamerikas erhältlich sind, erhalten Sie von Ihrem regionalen Verkaufsbüro. Kontaktinformationen finden Sie auf der Rückseite dieses Handbuchs.

Corporate PrimeSupport auf einen Blick

Feature	Knowledge Center	Connect	Priority	Enterprise
Technischer Support über Website	Ja	Ja	Ja	Ja
Softwareaktualisierungen	Ja	Ja	Ja	Ja
Technischer Support per Telefon	—	Montag bis Freitag 08:00 - 20:00 Uhr, amerikanische Zentralzeit	Montag bis Freitag 08:00 - 20:00 Uhr, amerikanische Zentralzeit Notfallbetreuung außerhalb der Geschäftszeiten	Rund-um-die-Uhr-Zugriff auf den Ihnen zugewiesenen Supportbetreuer an sieben Tagen der Woche
Bevorzugte Anrufbearbeitung	—	—	Ja	Ja
Support außerhalb der Geschäftszeiten	—	—	Ja	Ja
Speziell zugeteilter Mitarbeiter des Technischen Support	—	—	—	Ja
Aktiver Kontakt durch den Support	—	—	—	Ja
Benannte Kundenkontaktpersonen	—	—	—	Mindestens 5
Garantierte Antwortfristen	—	—	Innerhalb einer Stunde bei dringenden Problemen	Außerhalb der Geschäftszeiten über Pager 30 Minuten Voicemail: 1 Stunde Antwort auf eine E-Mail-Nachricht: 4 Stunden

PrimeSupport-Optionen für Privatkunden

Wenn Sie Ihr McAfee-Produkt bei einem Händler oder über die McAfee-Website erworben haben, sind auch einige Supportdienste im Lieferumfang enthalten. Die Stufe des jeweils eingeschlossenen Supports ist abhängig vom erworbenen Produkt. Zu den Diensten, die zu Ihrer Verfügung stehen, gehören u. a.:

- Kostenlose .DAT-Dateiaktualisierungen während der Lebensdauer des Produkts über die McAfee-Website, die AutoUpdate-Funktion des Produkts oder den SecureCast-Dienst (Einzelheiten finden Sie im Kapitel oder Anhang zur Softwareaktualisierung im *Benutzerhandbuch* Ihrer Virenschutzsoftware). Sie können Ihre Datendateien auch mit Hilfe Ihres Webbrowsers aktualisieren. Besuchen Sie hierzu:

  http://www.nai.com/asp_set/download/dats/find.asp

- Kostenlose Programmaktualisierungen (der ausführbaren Datei) für ein Jahr über die McAfee-Website, die AutoUpdate-Funktion des Produkts oder den SecureCast-Dienst (Einzelheiten finden Sie im Kapitel oder Anhang zur Softwareaktualisierung im *Benutzerhandbuch* Ihrer Virenschutzsoftware). Wenn Sie die Deluxe-Version eines McAfee-Produkts erworben haben, erhalten Sie für die Dauer von zwei Jahren kostenlos Programm-Upgrades. Sie können Ihre Datendateien auch aktualisieren, indem Sie hier unsere Website mit dem Webbrowser besuchen:

  http://www.nai.com/asp_set/download/upgrade/login.asp

- Rund um die Uhr an sieben Tagen die Woche freier Zugriff auf Support, online oder auf elektronischem Weg, durch das Sprach- und Faxsystem von McAfee, unsere Website und über andere Online-Dienste wie AOL und CompuServe.

  Um die elektronischen Dienste von Network Associates zu kontaktieren, wählen Sie eine der folgenden Optionen:

  – Automatisches Sprach- und Faxsystem: (408) 346-3414

  – McAfee-Website http://support.nai.com

  – CompuServe: GO NAI

  – AOL: Stichwort MCAFEE

- Kostenloser Zugriff auf die PrimeSupport KnowledgeBase: Online-Zugriff auf technische Lösungen in einer (durchsuchbaren) Knowledge-Base (Wissensdatenbank), elektronische Übermittlung von Ereignissen und technischen Dokumenten, darunter Benutzerhandbücher, Listen mit häufig gestellten Fragen und Antworten sowie Release Notes. Besuchen Sie die KnowledgeBase unter:

  http://knowledge.nai.com/

- Neunzig Tage zusätzlicher technischer Support von einem Supporttechniker von McAfee während der normalen Geschäftszeiten, Montag bis Freitag von 8:00 bis 20:00 Uhr amerikanische Zentralzeit.

Sie können auch eine Vielzahl weiterer Supportoptionen nutzen, die auf Ihre Bedürfnisse zugeschnitten sind. Sie können sich diese Optionen beim Kauf von McAfee-Produkten oder nach Ablauf des kostenlosen neunzigtägigen Supportzeitraums sichern:

- **Small Office/Home Office-Jahresplan.** Dieser Plan gewährt unbegrenzten, kostenlosen Technischen Support während der normalen Arbeitszeiten (Montag bis Freitag von 08:00 bis 20:00 amerikanische Zentralzeit).
- **Pay-Per-Minute-Plan.** Dieser Plan gewährt Support nur bei Bedarf: Zugriff auf den technischen Support über 0900-Nummer, bevorzugte Anrufbearbeitung zum Minimieren der Wartezeit und die ersten beiden Supportminuten gratis.
- **Online Upgrades-Plan.** Mit diesem Plan erhalten Sie die Möglichkeit über Online- oder elektronische Dienste von McAfee Produkt-Upgrades zu erhalten.
- **Quarterly Disk/CD-Plan.** Wenn Sie diesen Plan erwerben, erhalten Sie automatisch jedes Vierteljahr Upgrade-Disketten oder CDs, für den Fall, daß Sie keine Möglichkeit haben, Upgrades online abzurufen. Dieser Dienst ist nur für VirusScan und NetShield erhältlich.

Bestellen von Retail PrimeSupport

So bestellen Sie den PrimeSupport Small Office/Home Office Annual Plan, Pay-Per-Minute Plan, Online Upgrades Plan oder Quarterly Disk/CD Plan für Ihre McAfee-Produkte:

- Rufen Sie in Nordamerika den McAfee-Kundendienst unter (972) 278-6100 an; oder
- Besuchen Sie die McAfee-Website unter:

  http://www.nai.com/asp_set/services/prime_support/intro.asp

Beratung und Schulung bei McAfee

McAfee bietet Ihnen Beratung durch Fachleute und umfassende Weiterbildung, die dazu beiträgt, die Sicherheit und Leistungsfähigkeit Ihrer Netzwerkinvestitionen durch das McAfee Total Service Solutions-Programm zu maximieren.

Beratungsdienste durch Fachleute

Global Professional Services (Beratungsdienste durch Fachleute) von Network Associates stehen während aller Phasen des Wachstums Ihres Netzwerks zur Verfügung, von der Planung und Gestaltung über die Implementierung bis zur laufenden Verwaltung. Die Berater von Network Associates stellen fachkundige zusätzliche Ressourcen dar und sind eine unabhängige Instanz zur Lösung Ihrer Probleme. Sie erhalten Hilfe bei der Integration von Network Associates-Produkten in Ihre Umgebung sowie Unterstützung bei der Behandlung von Problemen oder Hilfe bei der Festlegung der Grundlagen der Netzwerkleistung. Darüber hinaus entwickeln und liefern die Berater von Network Associates Kundenlösungen, mit denen Sie Ihre Projektziele erfüllen, von langwierigen, extrem großen Implementationen bis hin zu kurzen Problemlösungssitzungen.

Schnelleinstiegdienste

Sie können verschiedene Schnelleinstiegdienste nutzen, die Sie bei der Implementierung eines neuen McAfee-Produkts unterstützen:

- **Basic and Advanced.** Dieser Dienst installiert, konfiguriert und optimiert Ihr neues McAfee-Produkt und versorgt das Personal mit Grundwissen über das Produkt.
- **Selfstart.** Dieser Dienst unterstützt Sie bei der eigenständigen Vorbereitung der Implementierung des neuen Produkts und installiert in einigen Fällen das Produkt.
- **Proposal Development.** Dieser Dienst wertet vor der Implementierung eines neuen Produkts Prozesse und Verfahren sowie Hardware- und Softwarevoraussetzungen aus, damit ein Berater Ihnen einen angepaßten Vorschlag vorbereiten kann.

Netzwerkberatung

Network Associates-Berater verfügen über Fachwissen für die Protokollanalyse und eine herstellerunabhängige Perspektive, die für unvoreingenommene Lösungen bei der Fehlerbehebung und eine Optimierung Ihres Netzwerks sorgt. Ferner beschleunigen ihre fundierten Kenntnisse zu optimalen Netzwerkverwaltungspraktiken sowie ihre Branchenbeziehungen die Problemidentifizierung und -behandlung.

Sie können eine Ihren Anforderungen entsprechende Beratung bestellen, die Sie bei Planung, Entwurf, Implementierung und Verwaltung Ihres Netzwerks unterstützt. Mit Hilfe der Berater können Sie die Auswirkungen des Einsatzes neuer Anwendungen, Netzwerkbetriebssysteme und Netzwerkverbindungssysteme einschätzen.

Wenden Sie sich an Network Associates Consulting Services unter der Rufnummer 1-800-395-3151 in den USA, um mehr über die verfügbaren Optionen zu erfahren, oder besuchen Sie die Network Associates-Website unter:

http://www.nai.com/asp_set/services/professional_services/professional_intro.asp

Total Education Services

Total Education Services von Network Associates vermitteln und optimieren die Fertigkeiten aller beruflich mit Netzwerken arbeitenden Personen durch praktische Unterweisungen, die sofort am Arbeitsplatz eingesetzt werden können. Die umfassenden Weiterbildungsdienste setzen im Bereich Technologie den Schwerpunkt auf das Management von Netzwerkfehlern und Netzwerkleistung und behandeln Problemlösungen auf allen Ebenen. Network Associates bietet auch Schulungen zu kleineren Produktmodulen an, damit Sie Leistungsmerkmale und Funktionalität Ihrer neuen Software verstehen.

Sie können sich ganzjährig an Kursen aus dem Total Education Services-Programm an den Network Associates-Schulungszentren einschreiben oder Kurse buchen, die speziell auf Ihre Erfordernisse abgestimmt sind und bei Ihnen im Hause durchgeführt werden. Alle Kurse vermitteln schrittweise das Wissen, mit dem Sie auf dem Weg des Lernens ein Höchstmaß an Fachwissen erreichen können. Network Associates ist Gründungsmitglied des Konsortiums Certified Network Expert (CNX).

Um mehr über diese Programme zu erfahren, wenden Sie sich an Network Associates Total Education Services unter der Rufnummer 1-800-395-3151 in den USA, oder besuchen Sie die Network Associates-Website unter:

http://www.nai.com/asp_set/services/educational_services/education_intro.asp

Index

Symbols

.CSV-Dateien, 251

.DAT-Dateien

- aktualisieren, 129
- Planen von Aktualisierungen, 269

.GSE-Konfigurationsdatei, 258

A

Administration (Registerkarte), 50, 113 to 114

Administratorhandbuch, 29

Aktionen, 229

- Ausweitungszeitraum, 236
- festlegen, 235
- Priorität, 237
- Reihenfolge, 237

aktiver Knoten

- auf einem Cluster Server, 253

aktualisieren

- Dienstprogramm Outbreak Manager, 226
- von v4.0.4 auf v4.5, 51

Aktualisieren von .DAT-Dateien

- Auswählen der zu aktualisierenden Server, 130
- Auswählen einer Aktualisierungsmethode, 132
- Termine, 136
- Verwenden des Internets, 133
- vom lokalen Computer aus, 138
- von einem Remote-Server, 134

Aktualisierung (Registerkarte), 131

- Clients aktualisieren, Option, 53

Alarmmeldungen

- Aktivieren und Deaktivieren, 182 to 183
- Ändern der Priorität, 184
- Anpassen, 182
- bei Virenepidemien, 233
- Programm starten als, 165
- Test fehlgeschlagen, 150
- Variablen in, 187

ALERT.TXT, 107

America Online (AOL)

- technischer Support über, xix, 278

andere Systemanforderungen, 32

Ändern

- Filter für das Dienstprogramm Quarantine Manager, 217

ändern

- Ausbruchparameter, 231
- Ausbruchregeln, 239
- Filter für das Dienstprogramm Log Manager, 198, 250
- Log Manager, Spaltensortierreihenfolge, 200 to 201
- Quarantine Manager, Spaltensortierreihenfolge, 221
- zu scannender Server, 98

Anfordern von Hilfe, 29, 48

Angeben neuer Namen für Ausbruchregeln, 241

Anlagenblockierung, 66 to 70

Anwesenheitszeiten, 223 to 224, 232

- festlegen, 233

Anzeigen

Spalten im Dienstprogramm Quarantine Manager, 219

anzeigen

Datensätze im Dienstprogramm Log Manager, 195, 251

Datensätze im Dienstprogramm Quarantine Manager, 220

Status der Ausbruchregeln, 242

Arbeiten mit

Dienstprogramm Outbreak Manager, 228

archivieren

Aktuelle Ansicht im Dienstprogramm Log Manager, 195, 251

Ansicht des Dienstprogramms Quarantine Manager, 212

Assistent

Outbreak Manager, 230

Update / Upgrade (Aktualisierung), 133

Auf Anforderung (Registerkarte), 72

Auf Anforderung-Bericht, 83

Auf Anforderung-Konsole, 89

Befehlszeilen-Scanoptionen, 100 to 103

Benutzeroberfläche, 91

Ergebnisfenster, 93

Ermitteln von Versionsinformationen, 98

Konfigurationsfenster, 96

Menüleiste

Ansicht, Menü, 92

Hilfe, Menü, 93

Menü „Datei“, 92

Scan, Menü, 92

Symbolleiste, 93

Überschreiben maximaler Sicherheitseinstellungen, 104

verwenden

aus dem Programmverzeichnis, 95

aus GroupShield-Eigenschaften, 94

Aufzeichnen

Aktivitäten im Zusammenhang mit Virusepidemien, 237

aufzeichnen

Aktivitäten im Zusammenhang mit Virusepidemien, 244

Ausbruch

Erkennen, 223

Log (Protokoll), 225, 237, 244

Regel, Ausweitungszeitraum, 236

ausführen

Dienstprogramm Outbreak Manager, 227

Auslöser

festlegen, 230

Parameter, 229

auswählen

Administratorpostfächer, 113

Anwesenheitszeiten, 233

Auswählen einer Isolierungsmethode, 116

Ausweitungszeitraum, 224, 236

Automatische

Aktionen, 224

Reaktionen, 223

AutoUpdate-Technologie

Inkrementelle .DAT-Aktualisierungen, 130, 266 to 269

AVERT Laboratories

Senden von Objekten an, 214

Avform, 47

B

Bearbeiten

Filter für das Dienstprogramm Quarantine Manager, 217
Parameter, 231
bearbeiten
Ausbruchregeln, 239
Filter für das Dienstprogramm Log Manager, 198, 250
Befehlszeile
Scanbeispiele, 103
Scannen auf Anforderung, 99
Scanoptionen, 100
Bei Zugriff (Registerkarte), 62
Bei Zugriff-Scannen
Aktionen bei Viruserkennung, 65
Auswählen von Scanoptionen, 62
Blockieren von Anlagen, 66
Benachrichtigung
Ändern der Standardnachricht, 111
bei Virusepidemien, 224
Einfügbare Ersatztexte, 112
Empfänger, 107
Nachricht
bei Virenepidemien, 232
per Alert Manager (Reaktion), 233
per E-Mail (Reaktion), 232
Benachrichtigung (Registerkarte), 110
Benennen von Ausbruchregeln, 238, 241
Benutzeroberfläche
Senden von Virusalarmmeldungen an Warnungs-Manager, 180 to 182
Beratungsdienste, 280
beschädigte Datei
reparieren, 54
Bildschirm
Aktualisierungs-Assistent
Aktualisierung konfigurieren, 135
Internet-Einstellungen, 133
Konfiguration geplanter Aktualisierung, 136
Auf Anforderung-Konsole
Einstellungen, 96
Outbreak Manager
Regelaktionen, 235
Regelauslöser, 230
Regelreaktionen, 231
Regelübersicht, 238
Windows Installer
Administrator-Setup, 39
Anwendung hinzufügen / entfernen, 55 to 56
Benutzerbenachrichtigungs-Setup, 41
Benutzerinformationen, 37
Deinstallation, Bildschirm, 57
Quarantäne-Setup, 40
Server-Setup, 37
Willkommen, 36
Zeitplan-Setup, 43
Zusammenfassung, 43
Windows NT
Systemsteuerung - Option „Dienste“, 49
Blockieren von Anlagen
nach Dateinamen, 68
nach Erweiterungstyp, 67
nach Größe, 69

C

Centralized Alerting (zentralisierte Warnungen)
Clusterressource, verwenden mit, 143

Clients aktualisieren, Option, 53
Cluster Server
aktualisieren, 254
der aktive Knoten, 253
Entfernen von GroupShield für Exchange, 256
zusätzliche Installationsinformationen, 255
Clusteradministrator, 254
CompuServe, technischer Support über, xix, 278

D

.DAT-Dateiupdates
Melden neuer Objekte für, xxi
Desktop Management Interface (DMI), als Warnmethode, 168 to 169
Dialogfeld
GroupShield-Systemmonitor
Diagramm erweitern, 202
Log Manager
Datensatzdetails, 196
Filterabfrage, 197
Filterabfrage, Filterobjekte, 197
Öffnen, 195
Spaltenanzeige, 200
Speichern unter, 194
Outbreak Manager, 228
Anwesenheitszeiten, 234
Datensatzdetails, 251
Filterabfrage, 249
Filterspalte, 249
Trigger Plugin, 244
Verfügbare Aktionen, 236
Quarantine Manager
Datensatzdetails, 220
Element filtern, 216
Filterabfrage, 216
Öffnen, 213
Spaltenanzeige, 219
Speichern unter, 212
Dialogfeld "Spaltenanzeige", 200
Dialogfeld „Anwesenheitszeiten“, 234
Dialogfeld „Datensatzdetails“, 196, 251
Dialogfeld „Filterabfrage“, 197, 249
Dialogfeld „Filterspalte“, 249
Dialogfeld „Outbreak Manager Trigger Plugin“, 244
Dialogfeld „Regelaktionen“, 235
Dialogfeld „Regelauslöser“, 230
Dialogfeld „Regelreaktionen“, 231
Dialogfeld „Regelübersicht“, 238
Dialogfeld „Verfügbare Aktionen“, 236
Dienste
anhalten und neu starten, 48
entfernen, 58
GroupShield für Exchange, 46
Dienstkonto, 31
Dienstprogramm Log Manager, 189, 237, 244
Aktualisieren der Ausgabe, 127
Aktuelle Ansicht archivieren, 195
Ändern der Spaltensortierreihenfolge, 200 to 201
Anfordern von Hilfe, 201 to 202
Anzeigen von Datensätzen, 195
Benutzeroberfläche, 127, 190
Dialogfeld "Spaltenanzeige", 200
Entfernen von Spalten aus der Ansicht, 200
Ereignisprotokollierungsoptionen, 126
Ergebnisfenster, 193, 248

Ermitteln von Versionsinformationen, 201
Filtern der Datenbank, 196, 248
Hinzufügen von Spalten zur Ansicht, 200
Menüleiste
Ansicht, Menü, 191
Hilfe, Menü, 192
Menü „Datei“, 190
Protokollierungsoptionen – Komponenten, 126
Speichern der Datenbank, 194
Symbolleiste, 192
Wechseln des Speicherorts, 128
Dienstprogramm Outbreak Manager, 223
Ändern Reihenfolge Regeln, 242
Ändern von Regeln, 239
anzeigen
Status der Ausbruchregeln, 242
Erstellen neuer Regeln, 229
Installationsanforderungen, 226
Installieren, Aktualisieren und Entfernen, 226
Kopieren von Regeln, 240
Löschen von Regeln, 239
öffnen, 227
Übernehmen Ihrer Änderungen, 229
Übersicht, 223
Umbenennen von Regeln, 241
verwenden, 228
Dienstprogramme, Registerkarte, 53
Dienstverweigerung
verhindern, 119
DMI, als Warnmethode, 168 to 169
Dokumente
Administratorhandbuch, 29
LICENSE.RTF, 30
Online-Hilfe, 29
README.RTF, 29
Drucker, als Warnmethode, 162 to 165
duplizieren
Ausbruchregeln, 240
Durchführen
Umfassende Protokollierung für Virenepidemieaktivitäten, 237

E

EICAR
European Institute of Computer Anti-virus Research, 43 to 44
Einfügbare Ersatztexte für Benachrichtigungen, 112
Einführung
Dienstprogramm Outbreak Manager, 223
GroupShield für Exchange, 27
Einrichten
Auslöser für eine Ausbruchregel, 230
elektronische Dienste, Kontaktaufnahme für technischen Support, 278
E-Mail
Adressen zum Melden neuer Viren an McAfee, xxi
als Warnmethode, 154 to 157
Benachrichtigung
bei Virenepidemien, 232
Entfernen
GroupShield für Exchange
mit Hilfe von Windows Installer, 56
GroupShield-Software von einem Cluster Server, 256
entfernen

Ausbruchregeln, 239

Datensätze aus dem Dienstprogramm Log Manager, 252

Dienstprogramm Outbreak Manager, 226

Filter für das Dienstprogramm Log Manager, 199, 250

Filter für das Dienstprogramm Quarantine Manager, 218

Log Manager-Spalten, 200

Quarantine Manager-Spalten, 219

Ereignisanzeige

Als Empfänger für Alarmmeldungen, 172 to 175

Ergebnisfenster

Dienstprogramm Log Manager, 193, 248

Quarantine Manager, Dienstprogramm, 210

Erhöhen Ihres Virenschutzes, 223

Erkennen von Virusepidemien, 223

Ersatz für Anlage, 107

Erstellen

Ausbruchregeln, 229

Filter für das Dienstprogramm Quarantine Manager, 215

erstellen

Filter für das Dienstprogramm Log Manager, 196, 249

Erweitern Ihres Virenschutzes, 223

F

Fehlerbehebung bei Fehlschlagen von Alarmmeldungstests, 150

festlegen

Aktionen für eine Ausbruchregel, 235

Anwesenheitszeiten, 233

Auslöser für eine Ausbruchregel, 230, 232

Filter für das Dienstprogramm Log Manager, 249

Neue Namen für Ausbruchregeln, 241

Reihenfolge Ausbruchregeln, 242

Filtern

Quarantine Manager, Dienstprogramm, 215

filtern

Dienstprogramm Log Manager, 196, 248

Funktionen des Dienstprogramms Outbreak Manager, 223

G

GroupShield für Exchange, 28

Add-Ins, 46

aktualisieren, 51

Auf Anforderung-Bericht, 83

Auf Anforderung-Konsole, 89

Dienste, 46

Dienstprogramm Log Manager, 189

einzurichtende Konten, 31

entfernen, 56

Entfernen von einem Cluster Server, 256

erwerben, 31

installieren

auf einem Microsoft Cluster Server, 253

auf mehreren Servern, 260

erforderliche Systemkonten, 31

im Hintergrund, 257

Systemanforderungen, 32

Komponenten

Auf Anforderung-Konsole, 28

Dienstprogramm Log Manager, 189

McAfee Log Manager, 28
McAfee Outbreak Manager, 28
McAfee Quarantine Manager, 28
McAfee Warnungs-Manager, 28
monitor, 28
Systemmonitor, 189, 202
Konfigurationsdatei, 258
Öffnen, 50
Organisationsformulare, 46 to 47
Quarantäneverzeichnis, 48
Quarantine Manager, Dienstprogramm, 48
reparieren, 54
Systemanforderungen, 32
für Hintergrundinstallation, 257
Installieren von GroupShield auf einem Cluster Server, 253
Systemmonitor, 189, 202
verborgene Empfänger, 46
Wichtigste Features, 30
zusammen mit anderer McAfee-Software, 70
GroupShield-Eigenschaften, 28
Administration (Registerkarte), 50, 113 to 114
Aktualisierung (Registerkarte), 131
Auf Anforderung (Registerkarte), 72
Bei Zugriff (Registerkarte), 62
Benachrichtigung (Registerkarte), 110
Dienstprogramme, Registerkarte, 53
Protokollierung (Registerkarte), 126
Verschlüsselung (Registerkarte), 120
Version (Registerkarte), 123
Zeitplanung (Registerkarte), 86

H

Heuristik
Makro, 62, 77
Programm, 62, 77
Hilfe
Beschreibung, 29
erhalten, 48
im Log Manager, 202
im Quarantine Manager, 222
Hintergrundinstallation der GroupShield-Software, 257
INSTMSIW.EXE-Datei, 258
Hintergrundinstallation GroupShield
Systemanforderungen, 257
Hintergrundinstallation von GroupShield
SETUP.MSI-Datei, 259
hinzufügen
Administratorpostfächer, 113
Ausbruchregeln, 229
Filter für das Dienstprogramm Log Manager, 196, 249
Filter für das Dienstprogramm Quarantine Manager, 215
geplanten Scanvorgang, 86
Log Manager-Spalten, 200
Quarantine Manager-Spalten, 219

I

identif.
Reihenfolge Ausbruchregeln, 242
Identifizieren
Virusepidemien, 223
identifizieren
Aktionen für eine Ausbruchregel, 235
Anwesenheitszeiten, 233

Auslöser für eine Ausbruchregel, 232

Info

Dienstprogramm Outbreak Manager, 223

GroupShield für Exchange, 27

Inkrementelles Scannen

Scanvorgänge auf Anforderung, 81

Installation

Änderungen an Ihrem System, 46

Anforderungen

für Dienstprogramm Outbreak Manager, 226

für einen Cluster Server, 253

für Hintergrundinstallation, 257

GroupShield für Exchange auf einem einzelnen Server, 32

auf einem einzelnen Microsoft Exchange-Server, 34

auf einem Microsoft Cluster Server, 253

auf mehreren Servern, 260

Hintergrundinstallation, 257

Schritte, 35 to 44

testen, 43 to 44

Installationscheckliste, 33

Installationskonto, 31

installieren

auf einem Microsoft Cluster Server, 253

auf mehreren Servern, 260

Bevor Sie beginnen, 33

Dienstprogramm Outbreak Manager, 226

im Hintergrund, 257

Interaktion zwischen dem Dienstprogramm Outbreak Manager und anderer Virenschutz-Software, 225

K

Komponenten, 28

konfig.

Reihenfolge Ausbruchregeln, 242

Konfigurationsdatei

verwenden zur Installation von GroupShield für Exchange auf mehreren Servern, 260

verwenden zur Installation von GroupShield im Hintergrund, 258

Konfigurieren

Auslöser für eine Ausbruchregel, 230

konfigurieren

Aktionen für eine Ausbruchregel, 235

Anwesenheitszeiten, 233

Auslöser für eine Ausbruchregel, 232

Neue Namen für Ausbruchregeln, 241

Kontextabhängige Hilfe, 29

kopieren

Ausbruchregeln, 240

Kundendienst

Kontaktaufnahme, xvii

L

LICENSE.RTF, 30

Log Manager, Dienstprogramm, 225

Löschen

Datensätze aus dem Dienstprogramm Log Manager, 252

Filter für das Dienstprogramm Quarantine Manager, 218

löschen

Ausbruchregeln, 239

Datensätze aus dem Dienstprogramm Log Manager, 252

Filter für das Dienstprogramm Log Manager, 199, 250

M

Manuelle Aktionen, 224

McAfee

Kontaktaufnahme

innerhalb der USA, xix

über America Online, xix

über CompuServe, xix

Log Manager, 189

Quarantine Manager, 48, 207

Warnungs-Manager, 141

McAfee-Aktualisierungsdienstprogramme für .DAT-Dateien

EXTRA.DAT, 265

SecureCast, 264

SuperDAT, 263

von .DAT-Dateiarchiven aus, 265

Melden von Viren, die von McAfee nicht entdeckt werden, xxi

Microsoft Exchange

Add-Ins, 46

Microsoft Exchange Administrator, 50

Microsoft Virus Scan-API, 27

Modem, Senden von Warnungen von mehreren Servern an einen Pager, 147

Modifizieren

Filter für das Dienstprogramm Quarantine Manager, 217

modifizieren

Ausbruchregeln, 239

Filter für das Dienstprogramm Log Manager, 198, 250

Parameter, 231

N

Network Associates

Beratungsdienste, 280

Kontaktaufnahme

außerhalb der USA, xxii

Kundendienst, xviii

Schulung, xx, 280

Supportdienste, 273

Website-Adresse für Software-Aktualisierungen und -Upgrade, 278

Weiterbildungsdienste, 281

Neue

Ausbruchregeln, 229

Neue Viren, melden an McAfee, xxi

Neusortieren Ausbruchregeln, 242

O

Öffnen

GroupShield für Exchange, 50

Quarantine Manager, Dienstprogramm, 211

Windows-Systemsteuerung, 49

öffnen

Auf Anforderung-Bericht, 84

Dienstprogramm Alert Manager, 144

Dienstprogramm Log Manager, 127

Dienstprogramm Outbreak Manager, 227

Quarantine Manager, Dienstprogramm, 116

Systemmonitor, 202

Online-Hilfe, 29

Organisationsformulare

Avform, 47

Sumform, 47

Outbreak Manager
Dialogfeld, 228
Symbol, 225
Outbreak Manager-Assistent, 230

P

Pager, als Warnmethode, 158 to 162
Parameter
ändern, 231
Auslöser, 229
Planen von .DAT-Dateiupdates, 136
PrimeSupport
Geschäftskunden
auf einen Blick, 277
bestellen, 276
Connect, 274
Enterprise, 275
KnowledgeCenter, 273
Priority, 274
Priorität
Ausbruchaktionen, 237
Ausbruchregeln, 242
Priorität von Ausbruchaktionen, 237
Priorität, Ausbruchaktionen, 237
Professional Consulting Services, Beschreibung, 280
Programm
starten
Als Reaktion auf eine Viruswarnung, 170 to 172
Protokollieren
Aktivitäten im Zusammenhang mit Virusepidemien, 225
protokollieren
Aktivitäten im Zusammenhang mit Virusepidemien, 237, 244
Protokollierung (Registerkarte), 126

Q

QNumber, 210
Quarantäne
Aktivieren und Deaktivieren des Features, 48
Auswählen einer Isolierungsmethode, 116
Optionen, 48
Verzeichnis, 222
Quarantine Manager, Dienstprogramm
Ändern der Spaltensortierreihenfolge, 221
Anfordern von Hilfe, 222
Anzeigen von Datensätzen, 220
Benutzeroberfläche, 116, 207
Ergebnisfenster, 210
Ermitteln von Versionsinformationen, 220
Hinzufügen von Spalten zur Ansicht, 219
Menüleiste
Ansicht, Menü, 208
Datei, Menü, 207
Hilfe, Menü, 209
Objekt, Menü, 208
Öffnen einer archivierten Datenbank, 213
Säubern infizierter Objekte, 215
senden
infizierte Objekte an Network Associates, 214
isolierte Objekte an andere Benutzer, 214
Speichern der Datenbank, 212
Symbolleiste, 209 to 210

Ticket-Nummer, 210
Verwenden, 211

R

README.RTF, 29
Reaktionen, 229
auf Virusepidemien, 223
festlegen, 232
Rechte and Berechtigungen, 31
Regel
Aktionen, 229
Status, 224
anzeigen, 242
Registerkarte
Administration, 50, 114
Aktualisierung, 131
Auf Anforderung, 72
Bei Zugriff, 62
Benachrichtigung, 110
Dienstprogramme, 53
Protokollierung, 126
Verschlüsselung, 120
Version, 123
Zeitplanung, 86
Registrierungsschlüssel
entfernen, 59 to 60
Reihenfolge
Ausbruchaktionen, 237
Ausbruchregeln, 242
Reparieren von GroupShield für Exchange, 54

S

Säubern infizierter Objekte, 215
Scannen auf Anforderung
Aktionen bei Viruserkennung, 79
Auswahl der zu scannenden Objekte, 72
Auswählen von Scanoptionen, 76
Beispiele für Befehlszeilen, 103
Inkrementelles Scannen, 81
Termine, 85
über die Befehlszeile, 99
Schulung für Network Associates-Produkte, xx
Termine, xx
Schulung für Virenschutzprodukte, 280
Schützen vor
Virusepidemien, 223
senden
infizierte Objekte per E-Mail, 214
Server
Enterprise, 32
Standard, 32
Simple Network Management Protocol (SNMP), als Warnmethode, 165 to 167
SNMP, als Warnmethode, 165 to 167
Software-Aktualisierungen und -Upgrades, Website-Adressen zum Abrufen von, 278
Speichern
Aktuelle Ansicht im Dienstprogramm Log Manager, 194, 251
Ansicht des Dienstprogramms Quarantine Manager, 212
Dienstprogramm Outbreak Manager, Änderungen, 229
speichern
Aktuelle Ansicht im Dienstprogramm Log Manager, 251
Ansicht des Dienstprogramms Quarantine Manager, 212
Dienstprogramm Outbreak Manager, Änderungen, 229

Starten
GroupShield für Exchange, 50
starten
Dienstprogramm Outbreak Manager, 227
Ein Programm als Reaktion auf eine Viruswarnung, 170 to 172
Scanvorgang, 94
Status der Ausbruchregeln, 224
anzeigen, 242
Sumform, 47
Support
Geschäftszeiten, 279
PrimeSupport für Geschäftskunden
auf einen Blick, 277
bestellen, 276
Connect, 274
Enterprise, 275
KnowledgeCenter, 273
Priority, 274
PrimeSupport für Privatkunden, 278 to 279
über elektronische Dienste, 278
Symbol
Auf Anforderung-Konsole, 96
Dienste, 49
Outbreak Manager, 225
Systemanforderungen, 32
Anforderungen für das Dienstprogramm Outbreak Manager, 227
Enterprise Server, 32
für einen Cluster Server, 253
Installieren GroupShield im Hintergrund, 257
Standardserver, 32
Systemmonitor, 189, 202

T

Technischer Support
E-Mail-Adresse für, xix
Geschäftszeiten, 279
Online, xix
PrimeSupport für Geschäftskunden
auf einen Blick, 277
bestellen, 276
Connect, 274
Enterprise, 275
KnowledgeCenter, 273
Priority, 274
Telefonnummern für, xix
über elektronische Dienste, 278
Vom Benutzer benötigte Informationen, xix
Terminal Server, Senden von Alarmmeldungen an Clients, 177 to 180
Testen (Schaltfläche), Alarmmeldung schlägt fehl, 150
Testen Ihrer Installation, 43 to 44
Ticket-Nummer, 107, 210
Ton, als Alarmmeldung, 175 to 177
Total Education Services, Beschreibung, 280
Total Service Solutions, Kontaktaufnahme, 280

U

Übernehmen Ihrer Änderungen
Dienstprogramm Outbreak Manager, 229
überprüfen
Status der Ausbruchregeln, 242
Übersicht
Dienstprogramm Outbreak Manager, 223

überwachen
E-Mail-Verkehr und Viruserkennung, 202
Umbenennen von Ausbruchregeln, 241
Umfassende Protokollierung für Virenepidemieaktivitäten, 237

V

verbergen
Spalten im Dienstprogramm Log Manager, 200
Spalten im Dienstprogramm Quarantine Manager, 219
verborgene Empfänger, 46
Verbreiten von Netzwerkmeldungen, 151 to 154
Verhindern einer Dienstverweigerung, 119
Verschlüsselte E-Mail
Optionen, 119
Verschlüsselung (Registerkarte), 120
Version (Registerkarte), 123
verwenden
Dienstprogramm Outbreak Manager, 228
Verwenden von Anwesenheitszeiten (Reaktion), 232
Viren
Melden neuer Arten an McAfee, xxi
Virenschutzsoftware
Melden neuer, von McAfee nicht entdeckter Viren, xxi
Virus
Ausbruchaktivität, 244
Epidemien
Schützen vor, 223
Virusepidemien, Schützen vor, 223
Vorhandene Ausbruchregeln, 239

W

Warnungs-Manager
Clusterressource
Konfigurieren als eine, 146
Verwenden von Zentrale Warnung mit, 143
öffnen, 144
Registerkarten
Centralized Alerting (zentralisierte Warnungen), 180 to 182
DMI, 168 to 169
Drucker, 162 to 165
E-Mail, 154 to 157
Netzwerkmeldung, 151 to 154
Pager, 158 to 162
Programm, 170 to 172
Protokollierung, 172 to 175
SNMP, 165 to 167
Terminal Server, 177 to 180
Ton, 175 to 177
Weiterleiten, 147 to 151
Zusammenfassung, 145
Verwenden zusammen mit dem Dienstprogramm Outbreak Manager, 233
.WAV-Datei, als Alarmmeldung, 175 to 177
Website, technischer Support von Network Associates über, 278
Weiterbildungsdienste, Beschreibung, 281
weiterleiten
infizierte Objekte per E-Mail, 214
Weiterleiten als Warnmethode, 147 to 151
Windows
Ereignisanzeige, als Empfänger für Alarmmeldungen, 172 to 175

Öffnen der
Windows-Systemsteuerung, 49

Systemmonitor, 202

Windows
2000-Installationsanforderungen, 32

Windows Installer

Clean Up-Dienstprogramm, 60

verwenden zum Entfernen der
GroupShield-Software von einem
Cluster Server, 256

Verwenden zum Entfernen von
GroupShield, 56

verwenden zur Installation der
GroupShield-Software im
Hintergrund, 258

Z

Zeit, Ausweitung, 236

Zeiten, Anwesenheitszeiten (Büro), 233

Zeitplanung (Registerkarte), 86

Zentrale Warnung

Einrichten, 180 to 182

Zusammenfassung (Seite),
Warnmethoden, 145